Thüringer Landesbeauftragter
für den **Datenschutz** und die **Informationsfreiheit**

2020

3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO | 2020

3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO:

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2020 bis 31. Dezember 2020
Zitiervorschlag: 3. TB DS-GVO LfDI Thüringen

Der 3. Tätigkeitsbericht DS-GVO steht im Internet unter www.tlfdi.de zum Abruf bereit.

Erfurt, im Oktober 2021

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort **9**

1. Schwerpunkte im Berichtszeitraum und Statistik 11

1.1 Schwerpunkte im Berichtszeitraum 11

1.2 Statistik im Berichtszeitraum 12

2. Themengebiete 15

2.1 Privacy-Shield durch Schrems II gekippt: Wie geht's weiter bei der Datenübermittlung in die USA 15

2.2 Die Corona-Pandemie und ihre Bewältigung bei Polizei und Kommunen 19

2.3 Corona und Schule 21

2.4 Corona-Warn-App 23

2.5 Thüringer Schulcloud 25

2.6 Einigung in der DSK nicht immer einfach 26

2.7 Windows 10 29

2.8 Digitale Souveränität 31

2.9 Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen 33

2.10 E-Mailverschlüsselung 34

2.11 Datenschutz-Folgeabschätzung (DS-FA) für den öffentlichen Bereich 37

2.12 Videokonferenzsysteme 39

2.13 Das Standard-Datenschutzmodell (SDM) – Version 2.0b 42

2.14 Smart-City 44

2.15 Zertifizierung – Quo vadis? 47

2.16 Irrtümer zur DS-GVO: Der TLfDI klärt auf 49

2.17 Ordnungswidrigkeitenverfahren beim TLfDI 52

2.18 Reichsbürger beim TLfDI: Wenn Argumente nicht mehr helfen 60

2.19 Datenpannen auch in Thüringen 63

2.20 Brexit – Über Nacht zum „datenschutzrechtlichen Drittstaat“ 65

3. Fälle öffentlicher Bereich 67

3.1 Weitergabe von Zeugendaten bei einem Verkehrsunfall 67

3.2 Polizeiliche Datenbanken – Zugriff nur aus dienstlichem Anlass 68

3.3 Predictive Policing – Kleine Anfrage 69

3.4 „Wer zeigt hier wen an?“ – Anzeigenaufnahme bei der Thüringer Polizei 70

3.5 Neufassung der Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung 72

3.6 Was hat der Gerichtsvollzieher zu tun – und darf ihn der TLfDI kontrollieren? 74

3.7 Sechstes Gesetz zur Änderung der Thüringer Kommunalordnung – Anhörungsverfahren vor dem Thüringer Landtag 77

3.8 Fehlerhaftes Update: Offenlegung von Kundendaten in einer Stadtbücherei 80

3.9 Umfrage zur Veröffentlichung von Jubiläen im Amtsblatt 81

3.10 Fehlversand von Mahnungen – auch ein Datenschutzproblem 86

3.11 (K)Ein Fall für kriminalistische Datenschützer: Patientenakten auf dem Friedhof 88

3.12 Infektionsschutz kontra Datenschutz, Kopie ja oder nein – Nachweis der Masernschutzimpfung in Kindergarten und Schule 90

3.13 Immer wieder die Frage: Was sind Sozialdaten? 92

3.14 Darf Personen das Fieber gemessen werden, bevor sie Zugang zu Geschäften oder anderen Einrichtungen bekommen? 93

3.15 Durchführung von Online-Prüfung an Hochschule 95

3.16 Distanzunterricht, was nun? Anforderungen an Videokonferenzsysteme 97

3.17 Maskenpflicht in der Schule – Schlagabtausch über Twitter auch in Thüringen 102

3.18 Umsetzen des Masernschutzgesetzes in der Schule 104

3.19 Vorlage des Steuerbescheides im Beihilfeverfahren 106

3.20 Umgang mit Personalakten zur Vorbereitung der Neugliederung kreisangehöriger Gemeinden 108

3.21 Veröffentlichung von Beschäftigtendaten auf der Internetseite 110

3.22 Was darf an personenbezogenen Daten außerhalb des behördlichen Arbeitsplatzes verarbeitet werden? Telearbeit und neue Formen des Arbeitens unter Corona 112

3.23 Vorgänge, die innerhalb der Bundesrepublik vom TLfDI an andere LfD's abgegeben wurden 114

3.24 Öffentlich bestellte Vermessungsingenieure (Sammelbeitrag) 116

4. Fälle nicht-öffentlicher Bereich 123

4.1 „Corona-Listen" 123

4.2 Frage nach personalisierten Reisegutscheinen 126

4.3 Coronabedingte Gutscheine bei Absagen von Veranstaltungen – bekommt man dennoch Geld ausgezahlt? (Überprüfung persönlicher Lebensumstände) 128

4.4 Wahlwerbung durch Versicherungsmakler (Verwarnung) 132

4.5 Beschwerde über einen Rechtsanwalt wegen Datenweitergabe ohne Einwilligung 134

4.6 Aufforderungs-E-Mails zur Bewertung eines Online-Shops bedürfen der Einwilligung des Betroffenen 136

4.7 WhatsApp-Adressdaten kontrollieren – über die Möglichkeiten von WhatsBox 139

4.8 Daten von Betreuten auf Abwegen 140

4.9 Beschwerde über offenen E-Mail-Verteiler 142

4.10 Ja, wo ist er denn...? Patient im Klinikum unauffindbar – wenn das elektronische Krankenhausinformationssystem Rätsel aufgibt 143

4.11 Datenschutz im Krankenhaus: Wenn der Expartner die Patientenakte „filzt“ 146

4.12 Datenschutz und Corona-Zeiten – Pseudonymisierung der Kontaktdaten 149

4.13 Wenn das Krankenhaus sagt: „Eine Kopie gibt's nie!“ ...dann hilft der TLfDI 150

4.14 Beschwerde über eine Pflegeeinrichtung wegen Veröffentlichung des Arbeitsvertrages in einer WhatsApp-Gruppe 152

4.15 Beschwerde über Fragebogen „betreutes Wohnen“ 153

4.16 Beschwerde gegen Vermieter wegen der unberechtigten Weitergabe einer Telefonnummer an den Handwerker 155

4.17 Datenerfassung bei Wohnungsbaugenossenschaft und Bonitätsauskunft bei Wohnungsanfragen 157

4.18 Vorlage des Personalausweises bei Immobilienkauf erst bei ernsthafter Kaufabsicht erforderlich 160

4.19 Übermittlung Mieterdaten an Grundversorger 162

4.20 Authentifizierung kann zwar lästig sein – notwendig ist sie doch 164

4.21 Wie löscht man sein Profil wieder von einem Portal? 165

4.22 Beschwerde über Nutzung von verlinkten Bildern bei Google 166

4.23 Beschwerde über eine Webseite wegen fehlender Datenschutzhinweise im Kontaktformular 167

4.24 Wenn der Arbeitgeber es gut meint, aber den Datenschutz außer Acht lässt 168

4.25 Erst AU-Bescheinigung – dann Kündigung: Ist das rechtens? Wie lange darf ein Arbeitgeber

Arbeitsunfähigkeitsbescheinigungen der Beschäftigten aufbewahren? 171

4.26 „Der gläserne Bauarbeiter“ – Angaben des Arbeitgebers über Beschäftigte zur Einhaltung des gesetzlichen Mindestlohnes 174

4.27 Big Brother beim Bratwurstessen 177

4.28 E-Mail-Kommunikation nur noch Ende-zu-Ende verschlüsselt? 180

4.29 Kleingartensiedlung unter Beobachtung 183

5. Entschließungen und Beschlüsse 186

5.1 Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie 186

5.2 Polizei 2020 – Risiken sehen, Chancen nutzen! 189

5.3 Registermodernisierung verfassungskonform umsetzen! 191

5.4 Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig! 193

5.5 Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen 195

5.6 Datenschutz braucht Landgerichte auch erstinstanzlich 199

5.7 Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen 201

5.8 Betreiber von Webseiten benötigen Rechtssicherheit Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen 204

5.9 Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten 207

5.10 Einwilligungsdokumente der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung 209

5.11 Vorabwidersprüche bei StreetView und vergleichbaren Diensten 211

5.12 Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich 212

5.13 Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie 220

5.14 Anwendung der DS-GVO auf Datenverarbeitungen von Parlamenten 234

5.15 Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise 235

6. Vorträge und Veranstaltungen 257

7. Anhang 261

7.1 Vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich – Entwurf des Brexit-Abkommens bietet viermonatige Übergangsfrist ab dem 1. Januar 2021 261

Stichwortverzeichnis 262

Vorwort

Dr. Lutz Hasse

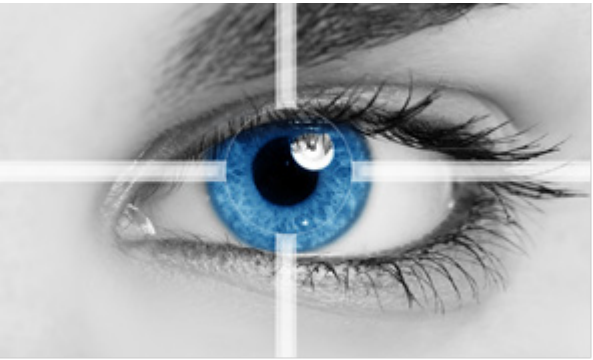
Zwar wird der Bericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nun im Jahresturnus veröffentlicht, man kann aber nicht sagen, dass alles ist wie immer. Die Corona-Pandemie hat auch die Arbeit des TLfDI maßgeblich bestimmt. Auf der einen Seite waren sehr viele datenschutzrechtlich Verantwortliche in Thüringen vor die Herausforderung gestellt, Datenverarbeitungen auf einmal digital durchführen zu müssen. Angefangen von Unterricht in der Schule über digitale Plattformen, dem mobilen Arbeiten über Telearbeit über die Notwendigkeit der Durchführung von Videokonferenzen, weil Treffen nur über die Distanz möglich sind, hin zu der Frage, wer Coronalisten einsehen und nutzen darf. Der TLfDI sah sich im Berichtszeitraum zahlreichen Anfragen zu datenschutzkonformen Lösungen der auftretenden praktischen Probleme gegenüber. Auf der anderen Seite musste auch der TLfDI seine Arbeit als Aufsichtsbehörde an die Anforderungen des Infektionsschutzes anpassen. Vororttermine waren so gut wie nicht mehr möglich und auch Termine mit Beschwerdeführern oder Zeugen in Bußgeldverfahren mussten sich auf das Allernotwendigste beschränken. Die Möglichkeit der Telearbeit wurde für die Beschäftigten der Behörde deutlich ausgeweitet. Meine Mitarbeiterinnen und Mitarbeiter haben diese herausfordernde Zeit mit großem Engagement gemeistert, wofür ich ihnen meine Hochachtung aussprechen möchte. Trotz der widrigen Umstände gab es auch in diesem Jahr Fortbildungs- und Informationsveranstaltungen

und etliche Veröffentlichungen rund um aktuelle datenschutzrechtliche Fragen. Einzelheiten dazu finden Sie in dem Bericht, der eine Auswahl der Themen enthält, die uns im Jahr 2020 beschäftigt haben.

Ich wünsche Ihnen ein interessantes Lesevergnügen mit nützlichen Einsichten.

Ihr
Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit.

1. Schwerpunkte im Berichtszeitraum und Statistik



© Minerva Studio - Eye close-up - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum

Die Arbeit des TLfDI im Berichtszeitraum war in zweierlei Hinsicht maßgeblich durch die Anforderungen der Corona-Pandemie geprägt. Einerseits galt es, die Aufgaben nach der DS-GVO auch unter erschwerten Bedingungen wahrnehmen zu können, andererseits gab es zahlreiche datenschutzrechtliche Probleme im Umgang mit der Pandemie.

Angesichts der Corona-Pandemie im Jahr 2020 trat eine sehr wichtige Entscheidung, die der Europäische Gerichtshof (EuGH) zu Datenübermittlungen in die USA traf, fast in den Hintergrund. Dies ist angesichts der Bedeutung des Urteils in der Rechtssache C-311/18 „Schrems II“ nicht gerechtfertigt. Personenbezogene Daten von EU-Bürgern dürfen nur an Drittländer außerhalb des Europäischen Wirtschaftsraums übermittelt werden, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der Europäischen Union. Dies hat der EuGH für die USA verneint. Diese Entscheidung hat erhebliche Auswirkungen für Verantwortliche in Europa (siehe Beitrag 2.1). Mit ihr hängt auch mittelbar die Frage zusammen, inwieweit Produkte der Firma Microsoft, die bei etlichen Verantwortlichen nicht mehr wegzudenken sind, zum Einsatz kommen dürften (siehe Beitrag 2.7).

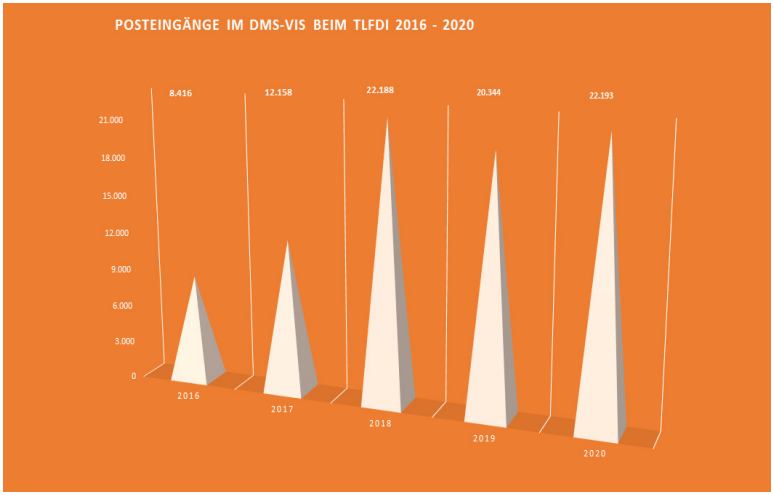
Ansonsten finden sich im Tätigkeitsbericht etliche Beiträge zu den datenschutzrechtlichen Auswirkungen der Corona-Pandemie. Sie hatte zur Folge, dass es im Berichtszeitraum so gut wie keine Vororttermine mehr gab und Beratungs- oder Schulungstermine nur online abgehalten werden konnten. Auch beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde die Telearbeit ausgebaut, um der Ansteckungsgefahr für seine Mitarbeiter möglichst effektiv zu begegnen.
Einen großen Raum nahm die Beratung der Verantwortlichen im Umgang mit der Pandemie in datenschutzrechtlicher Hinsicht ein. Ganz besonders betraf dies den schulischen Bereich, in dem innerhalb von kürzester Zeit von Präsenz- auf Digitalunterricht umgestellt werden musste, ohne dass die dafür erforderliche Infrastruktur vorhanden war (siehe Beitrag 2.3 und 2.5). Allerorts war der Bedarf an der Nutzung von Videokonferenzsystemen groß, der Datenschutz fand dabei zunächst kaum Beachtung (siehe Beitrag 2.12 und 3.16). Die Maskenpflicht an Schulen (siehe Beitrag 3.17) war ebenso Thema wie der Umgang mit Coronalisten (siehe Beitrag 4.1).
Nach wie vor war auch die Aufklärung und Sensibilisierung ein wichtiger Baustein der Arbeit des TLfDI mit Vorträgen und Veranstaltungen (siehe Beitrag 6) und Veröffentlichungen zu Datenschutzthemen, beispielsweise zu Datenschutzanforderungen für öffentliche Stellen (siehe Beitrag 2.9) und Datenschutz-Folgenabschätzung (siehe Beitrag 2.11).
Daneben gab es auch ansonsten zahlreiche Beschwerden und Beratungsanfragen (siehe Beitrag 1.2), von denen der Tätigkeitsbericht Ihnen einen repräsentativen Eindruck vermitteln soll. So gibt es beispielsweise immer noch zahlreiche Fälle, in denen die Zulässigkeit des Einsatzes von Videoüberwachungstechnik zu prüfen ist, es werden hierzu aber nur Beispielsfälle aufgeführt. Über alle Einzelfälle zu berichten, würde seine Kapazitäten sprengen und zu Lasten der Handlungsfähigkeit gehen. Die Auswahl der Beiträge soll Ihnen einen Eindruck von der Vielfältigkeit der vom TLfDI bearbeiteten Fälle geben.

1.2 Statistik im Berichtszeitraum

Auch im zweiten Kalenderjahr nach dem Wirksamwerden der DS-GVO ist die Zahl der Posteingänge beim TLfDI auf bisher höchstem Niveau. Meldungen von Datenpannen sowie auch der Eingang von

Beschwerden haben gegenüber dem letzten Berichtsjahr zugenommen.

Im Jahr 2020 gab es 22.193 Posteingänge beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Damit bewegt sich ihre Zahl mit einer Steigerung gegenüber dem Vorjahr auf dem höchsten Niveau seit Bestehen der Behörde.



Davon waren 3.058 Eingänge solche in Beschwerdeverfahren nach Art. 77 Datenschutz- Grundverordnung (DS-GVO), also Beschwerden von natürlichen Personen, die von der in Rede stehenden Datenverarbeitung **persönlich betroffen** sind. Über 6.800 Eingänge gab es im europäischen Kontext (unter anderem länderübergreifende Verfahren, Abstimmungsbedarfe mit Blick auf EuGH-Schrems-II und den Europäischen Datenschutzausschuss).
Ein Schwergewicht der Posteingänge liegt bei Anzeigen, Hinweisen, Beratungsanfragen und Abstimmungsverfahren zwischen den Datenschutzbeauftragten zu Fragen der Datenschutzkonferenz.
Insgesamt gab es zudem 204 Meldungen nach Art. 33 DS-GVO zu Verletzungen des Schutzes personenbezogener Daten. Hier ist eine deutliche Steigerung gegenüber dem Vorjahr mit 159 Meldungen zu verzeichnen. Es gab sehr viele Fälle, in denen E-Mails oder auch

Briefe an den falschen Adressaten versandt wurden. In manchen Fällen kam es zum Verlust von Akten oder sonstigen Papieren aufgrund von Unachtsamkeit oder Diebstahl. Es gab unberechtigte Zugriffe, Phishing-Angriffe und etliche Cyber-Angriffe. Wie der TLfDI in solchen Fällen verfährt, können sie dem Beitrag 2.19 entnehmen.
Im Berichtszeitraum wurden beim TLfDI 121 Bußgeldverfahren eröffnet. Insgesamt wurden 41 Bußgeldbescheide erlassen – hier hat sich die Zahl gegenüber dem Vorjahr fast verdoppelt – von denen 33 rechtskräftig sind. Gegen die übrigen acht Bescheide wurde Einspruch eingelegt. Davon liegen fünf Fälle dem Amtsgericht Erfurt zur abschließenden Entscheidung vor und zwei Bescheide wurden nach Prüfung der Einspruchsbegründung zurückgenommen. Ein Verfahren betraf Art. 83 Abs. 4 DS-GVO und 21 Verfahren Art. 83 Abs. 5 DS-GVO. Ein Verfahren wurde nach § 43 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz eingeleitet und 18 Verfahren betrafen § 43 Bundesdatenschutzgesetz (alte Fassung). Die Gesamthöhe der verhängten Bußgelder belief sich auf 17.630,00 Euro. Der Bußgeldrahmen der in 2020 erlassenen Bußgeldbescheide lag zwischen 50 Euro und 2.000 Euro.
Von den 41 Bußgeldbescheiden wurden 12 Bußgeldbescheide wegen unzulässiger Videoüberwachung und 13 Bußgeldbescheide gegen Polizeibeamte (wegen unbefugten Abrufen aus polizeilichen IT-Systemen und/oder der Übermittlung dienstlicher Daten über WhatsApp) erlassen. Weitere Einzelheiten zu Bußgeldverfahren beim TLfDI finden sich im Beitrag 2.17.
Nicht zu vergessen sind die zahlreichen Telefonate, die die Mitarbeiterinnen und Mitarbeiter des TLfDI täglich geführt haben, um Bürgerinnen und Bürger oder Verantwortliche telefonisch zu beraten. Viele Thüringer wählen diesen Weg, um sich über Datenschutzfragen (vorab) zu informieren. Nach einer überschlägigen Schätzung handelt es sich dabei um mindestens 25.000 Telefonate im Berichtszeitraum. Sie wurden aus Gründen der Arbeitsersparnis und der Vermeidung von Mitarbeiterüberwachung nicht erfasst.

2. Themengebiete

© Spencer- 3D Man Office - fotolia.com

2.1 Privacy-Shield durch Schrems II gekippt: Wie geht's weiter bei der Datenübermittlung in die USA

Der EuGH erklärte in seinem „Schrems II-Urteil" das Privacy Shield mit sofortiger Wirkung für unwirksam, weil das durch den EuGH bewertete US-Recht kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist. Nun stellt sich die Frage, unter welchen Voraussetzungen Datenübermittlungen in die USA möglich sind.

Nach der Datenschutz-Grundverordnung (DS-GVO) dürfen personenbezogene Daten von EU-Bürgern nur an Drittländer außerhalb des Europäischen Wirtschaftsraums übermittelt werden, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18 „Schrems II" (https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18) klargestellt, dass für die USA ein solches angemessenes Schutzniveau nicht besteht. Derartige Datenübermittlungen wurden bislang auf das

EU-US Privacy Shield-Abkommen, einem Angemessenheitsbeschluss der Europäischen Kommission, gestützt. Der EuGH erklärte das Privacy Shield mit sofortiger Wirkung für unwirksam, weil das durch den EuGH bewertete US-Recht kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist.
Dafür wurden unter anderem folgende Gründe angeführt:
Die Gesetze, auf deren Grundlage amerikanische Sicherheitsbehörden auf die in die USA übermittelten personenbezogenen Daten zugreifen können, verstoßen gegen die EU-Grundrechtecharta, da der Zugriff auf die personenbezogenen Daten von Nicht-Amerikanern nicht beschränkt wird und sie keine durchsetzbaren Rechte gegen etwaige Zugriffe haben. Weitere Informationen zum Inhalt der Entscheidung des EuGHs finden Sie unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/EU_UN/Kernaussagen-Schrems-II.pdf;jsessionid=B784CEB9397CB49731A2292E74523D26.intranet222?__blob=publicationFile&v=4.
Diese Entscheidung hat innerhalb der EU für einigen Wirbel gesorgt, finden doch täglich unzählige Datenübermittlungen aus der EU in die USA statt. Sei es beispielsweise beim Support technischer Geräte im Krankenhaus, bei der Nutzung von Telefonanlagen oder von Software amerikanischer Hersteller. Können nun keine Datenübermittlungen in die USA mehr stattfinden? Grundsätzlich sind nur unter den sehr restriktiven Voraussetzungen des Art. 49 DS-GVO Übermittlungen von personenbezogenen Daten in so genannte Drittländer möglich. Angesichts der Entscheidung des EuGHs müssen die Verantwortlichen aber tätig werden:
Jeder Verantwortliche im Sinne des Datenschutzrechts war jetzt aufgerufen, seine Datenübermittlungen in die USA zu überprüfen.
Datenübermittlungen in die USA, die bisher auf das EU-US Privacy Shield gestützt wurden, müssen nun durch eine Schutzmaßnahme nach Art. 46 DS-GVO abgesichert werden. Der EuGH hat die Verantwortung des Datenexporteurs hervorgehoben, für jede Datenübermittlung das Schutzniveau im Drittland zu prüfen und geeignete Garantien für den Schutz der in ein Drittland übermittelten Daten vorzusehen. Wenn der Schutz der übermittelten Daten auch durch zusätzliche Maßnahmen nicht hinreichend sichergestellt werden kann, ist die Datenübermittlung auszusetzen.
Nach dem Urteil des EuGHs hat der Europäische Datenschutzausschuss (EDSA) nach einer ersten Stellungnahme zentrale Fragen und

Antworten (FAQ) zur Umsetzung des Urteils veröffentlicht. Der deutsche Text der FAQ ist unter https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_de.pdf zu finden. Dieses Dokument soll Antworten auf einige häufig gestellte Fragen geben, die bei den Datenschutzaufsichtsbehörden eingehen.
Die FAQs legen dar, dass die Frage, ob personenbezogene Daten auf der Grundlage von **Standardvertragsklauseln** in die USA übermittelt werden dürfen oder nicht, vom Ergebnis der Prüfung des Verantwortlichen abhängt. Etwaige zusätzliche Maßnahmen müssen zusammen mit den Standardvertragsklauseln nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das gewährleistete angemessene Schutzniveau nicht beeinträchtigt. Eine kaum erfüllbare Aufgabe. Wenn durch einen Verantwortlichen mit einem Unternehmen in den USA verbindliche interne Datenschutzvorschriften (so genannte **Binding Corporate Rules**, „BCR“) verwendet werden, gelten die gleichen Grundsätze. Es ist daneben nach wie vor möglich, Daten aus dem Europäischen Wirtschaftraum in die USA auf der Grundlage der in Art. 49 DS-GVO vorgesehenen sehr restriktiven Ausnahmeregelungen zu übermitteln, sofern die dort festgelegten Bedingungen erfüllt sind. Der EDSA verweist auf seine Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung (EU) 2016/679. Insbesondere erinnert der EDSA daran, dass bei Übermittlungen, die auf der Grundlage der Einwilligung der betroffenen Person beruhen, bestimmte Bedingungen gelten. Die Einwilligung muss ausdrücklich sein, für den bestimmten Fall der betreffenden Datenübermittlung erteilt werden und in Kenntnis der Sachlage erfolgen, insbesondere, was die möglichen Risiken der Übermittlung betrifft. Die betroffene Person muss auch über die spezifischen Risiken unterrichtet werden, die sich daraus ergeben, dass ihre Daten in ein Land übermittelt werden, das keinen angemessenen Schutz bietet. In Bezug auf Übermittlungen, die für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich sind, ist zu berücksichtigen, dass personenbezogene Daten nur dann übermittelt werden dürfen, wenn die Übermittlung nur gelegentlich erfolgt.
Der EDSA weist auch auf die Schlüsselrolle der Aufsichtsbehörden bei der Durchsetzung der Datenschutz-Grundverordnung hin. Er beschäftigte sich weiterhin mit den Auswirkungen des Urteils und veröffentlichte am 11. November 2020 zwei Empfehlungen zur datenschutzrechtlichen Beurteilung von Datentransfers in Drittstaaten.

- In den „Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“ (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf) über Maßnahmen zur Gewährleistung des EU-Schutzniveaus bei der Übertragung von personenbezogenen Daten, ein Entwurf, der bis zum 30. November 2020 für Kommentare der Öffentlichkeit offenstand und noch nicht verabschiedet wurde und den
- „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf) zu den europäischen wesentlichen Garantien für Überwachungsmaßnahmen.

Am 12. November 2020 veröffentlichte die EU-Kommission ihren Entwurf für Standardvertragsklauseln (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries), der ebenfalls die Schrems II-Entscheidung berücksichtigt.

Im ersten Dokument wird ausführlich beschrieben, wie Unternehmen beurteilen und dokumentieren sollten, unter welchen Bedingungen die Übermittlungen personenbezogener Daten in Drittstaaten nach der Schrems II-Entscheidung durchgeführt werden können. Das Dokument lag im Berichtszeitraum noch nicht in der verbindlichen Endfassung vor. Über die dort festgelegten Maßnahmen wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) daher im nächsten Tätigkeitsbericht weitere Ausführungen machen.

Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder war nicht untätig. Sie richtete eine **Task Force** „Schrems II" ein, in der auch der TLfDI Mitglied ist. Aufgabe dieser Task Force ist es, unter anderem eine Strategie sowie konkrete Vorschläge für ein gemeinsames Vorgehen der deutschen Aufsichtsbehörden zur Umsetzung des EuGH-Urteils „Schrems II" zu erarbeiten (vergleiche https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf). Über die erzielten Ergebnisse, die sicherlich von einiger Brisanz sein werden an-

gesichts der entsprechenden Datenflüsse von global Playern, wird der TLfDI ebenfalls im nächsten Tätigkeitsbericht informieren.

2.2 Die Corona-Pandemie und ihre Bewältigung bei Polizei und Kommunen

Für jede Datenübermittlung als Unterform der Datenverarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO bedarf es einer Rechtsgrundlage. Konkret ging es um die Frage, wann und unter welchen Voraussetzungen die Gesundheitsämter personenbezogene Daten von Corona-Patientinnen und -Patienten sowie von den oben genannten Krankheitsverdächtigen an die Polizeibehörden übermitteln dürfen. Dem TLfDI wurden aber auch Fallkonstellationen bekannt, in denen weder diese noch andere Rechtsgrundlagen die Übermittlung von personenbezogenen Daten der Corona-Patienten und -Krankheitsverdächtigen an öffentliche Stellen rechtfertigten.

Die Corona-Pandemie, der Umgang mit ihr und ihre Bewältigung waren das große Thema, das den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ab März 2020 in seiner täglichen Arbeit intensiv beschäftigte. Auch für den TLfDI waren neben den Normen aus dem Infektionsschutzgesetz (IfSG) auch Begriffe wie Reproduktionswert (R-Wert), Inzidenzwert oder AHA-Regeln „Neuland“, mit denen sich seine Mitarbeiterinnen und Mitarbeiter erst einmal vertraut machen mussten.
Mit dem ersten „Lock down“ (also dem Herunterfahren des öffentlichen Lebens) und steigenden Infektionszahlen erreichten den TLfDI dann mehr und mehr Anfragen, wie und wem die personenbezogenen Daten von Personen, die positiv auf das Corona-Virus getestet wurden, und von Personen, die Krankheitsverdächtige im Sinne des § 2 Nr. 5 IfSG waren, übermittelt werden durften.
Der TLfDI informierte dazu bereits Anfang März 2020 die Landespolizeidirektion und die ihr nachgeordneten Polizeidienststellen sowie die Gesundheitsbehörden. Konkret ging es um die Frage, wann und unter welchen Voraussetzungen die Gesundheitsämter personenbezogene Daten von Corona-Patientinnen und -Patienten sowie von den oben genannten Krankheitsverdächtigen an die Polizeibehörden übermittelt werden dürfen. Der TLfDI wies darauf hin, dass, soweit Polizeivollzugsbeamte zu präventiven/repressiven Einsätzen in die Wohnung von Krankheitsverdächtigen gerufen werden, ihnen **im Einzel-**

fall auch – mangels spezieller Rechtsgrundlagen – gemäß Art. 9 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 16 Abs. 2 Nr. 1, 1. und 2. Variante Thüringer Datenschutzgesetz (ThürDSG) die insoweit erforderlichen personenbezogenen Daten dieser Corona-Patienten und -Krankheitsverdächtigen von den zuständigen Gesundheitsämtern übermittelt werden dürfen. Der TLfDI begründete seine Rechtsauffassung mit den folgenden zwei Argumenten:
Erstens: Diese Datenübermittlung an die Polizeibehörden war und ist für die Abwehr erheblicher Nachteile für das Gemeinwohl gemäß § 16 Abs. 2 Nr. 1, 1. Variante ThürDSG erforderlich. Die Übermittlung der personenbezogenen Daten von Corona-Kranken und -Verdächtigen dient ferner der Verhinderung der ungehinderten und schnellen Weiterverbreitung des Corona-Virus in der Bevölkerung.
Zweitens: Zum anderen dient die Übermittlung dieser personenbezogenen Daten an die Polizei dazu, dass die Gesundheit der Polizistinnen und Polizisten, die über den Begriff der subjektiven Rechtsgüter unter den Schutzbereich der öffentlichen Sicherheit fällt, geschützt wird. Deshalb war und ist auch § 16 Abs. 2 Nr. 1, 2. Variante ThürDSG als Rechtsgrundlage für diese Datenübermittlung einschlägig.
Abschließend wies der TLfDI die Polizei und die Gesundheitsbehörden noch darauf hin, dass in diesem Zusammenhang stets auch Art. 5 Abs. 1 Buchstabe c) DS-GVO zu beachten ist und personenbezogene Daten und ihre Übermittlung auf das für den Zweck der Datenverarbeitung notwendige Maß zu beschränken sind.
Im Anschluss daran sind dem TLfDI für den Berichtszeitraum keine Klagen über unzulässige Datenübermittlungen seitens der Gesundheitsämter an die Polizei bekannt geworden.
Ganz anders hatte der TLfDI dagegen den folgenden, kuriosen Corona-Datenschutzfall zu beurteilen: Die Datenschutzbeauftragte einer Kommune fragte beim TLfDI nach, ob das Gesundheitsamt die personenbezogenen Daten von Corona-Patienten und -Verdächtigen auch an den kommunalen Entsorgungsbetrieb übermitteln dürfte, da sich ja auch die Mitarbeiterinnen und Mitarbeiter der Müllentsorgung vor dem Corona-Virus schützen müssten. Der TLfDI antwortete der Datenschutzbeauftragten, dass er keine Gefahr im Sinne des § 54 Nr. 3 Ordnungsbehördengesetz für die Mitarbeitenden der Müllentsorgung erkennen könne und ferner eine solche Datenübermittlung auch nicht erforderlich im Sinne des Verhältnismäßigkeitsprinzips sei. Denn die Mitarbeitenden der Müllentsorgung hätten genügend andere Schutz-

maßnahmen zur Verfügung (Kleidung, Handschuhe et cetera), um sich vor der fernliegenden Wahrscheinlichkeit der Ansteckung mit Corona-Viren am und im Hausmüll zu schützen.

2.3 Corona und Schule

Die Corona-Pandemie stellt die Schulen vor die besondere Aufgabe, im Distanzunterricht den Schülerinnen und Schülern Wissen zu vermitteln und auch gleichzeitig die Klassengemeinschaft zu erhalten. Trotzdem müssen elementare datenschutzrechtliche Vorschriften beachtet werden. Vor der Nutzung von digitalen Medien für den Unterrichtseinsatz ist eine entsprechende kritische Prüfung unumgänglich.

Bereits im Jahr 2020 war der Schulbereich von den mit der Covid-19-Pandemie einhergehenden Kontaktverboten betroffen. Schnell war klar, dass mit den erforderlich gewordenen Schulschließungen eine Unterrichtung aller Schülerinnen und Schüler nur über Fernunterricht oder Lernen zu Hause („Homeschooling“) ermöglicht werden konnte. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beschäftigte sich aber bereits weit vor dem Ausbruch der Pandemie mit digitalen Lernformen. Der TLfDI erinnert an die gemeinsam mit anderen Landesdatenschutzbeauftragten bereits Anfang 2018 (!) erarbeitete Orientierungshilfe für Onlineplattformen im Schulunterricht oder sein Engagement bei der datenschutzrechtlichen Begleitung der Schul-Cloud des Hasso-Plattner-Instituts, die die Basis der in vielen Thüringer Schulen genutzten Thüringer Schulcloud bildet seit dem Jahr 2017. Trotzdem fiel der gesamte Kultusbereich – und dies nicht nur in Thüringen – aus allen Wolken, als die Situation dann wegen der Covid-19-Pandemie sehr akut wurde und Lösungen kurzfristig gefunden werden mussten. Woran von den Verantwortlichen nicht oder nur sehr vereinzelt gedacht wurde, war die Einhaltung der gesetzlich vorgegebenen Regelungen zu Datenschutz und Datensicherheit. Eine der wesentlichen Aufgaben des TLfDI ist es aber nun mal, alle Regelungen, die die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützen, zu überwachen. „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht“ (Erwägungsgrund 1 der Datenschutz-Grundverordnung). Ein solches Grundrecht kann selbstverständlich nicht aufgegeben werden, weil aus verschiedenen Gründen datenschutzrechtlich als mangelhaft

zu bezeichnende digitale Medien als Ersatz des Präsenzbetriebs in vielen Schulen zum Einsatz kommen. Für den TLfDI bedeutete die Pandemie eine Vervielfachung von Anfragen und Beschwerden an ihn aus dem Kreis von Schulleitungen, Lehrkräften, Eltern, Schülerinnen und Schülern. Außer der Beantwortung von Fragen stand der TLfDI auch für Beratung beim Einsatz bestimmter Schulsoftwaresysteme zur Verfügung oder gab Anregungen, welche Verfahren wie zu nutzen sind oder eben auch nicht. Da viele der Anfragen gleiche Sachverhalte betrafen, hatte das Thüringer Ministerium für Bildung, Jugend und Sport unter Mitarbeit des TLfDI eine ausführliche FAQ-Liste für Lehrkräfte erstellt, die ständig aktualisiert wird.
Der TLfDI musste oftmals in Erinnerung rufen, dass die Schulleitung die datenschutzrechtliche Verantwortung für alle schulisch eingesetzten digitalen Lernplattformen, Videokonferenzsysteme, Messenger-Dienste und weiterer Schulsoftware trägt. Dies ist auch bei der Nutzung der Thüringer Schulcloud oder des dienstlichen E-Mail-Accounts der Fall. Selbstverständlich muss die Schule als verantwortliche Stelle auch hierbei die geeigneten Maßnahmen nach Art. 12 Datenschutz-Grundverordnung (DS-GVO) treffen, um den betroffenen Schülerinnen, Schülern und deren Eltern alle Informationen gemäß den Artikeln 13 und 14 DS-GVO und alle Mitteilungen nach den Artikeln 15 bis 22 DS-GVO, also zum Beispiel Auskunfts-, Berichtigungs- und Löschungsrechte der Betroffenen und so weiter, zu übermitteln. Besonders kritisch waren Eigeninitiativen von Lehrkräften zu sehen, die ohne Zustimmung der Schulleitung Messenger-Dienste oder Schulsoftware bei ihren Schülerinnen und Schülern einsetzen. In solchen Fällen musste der TLfDI prüfen, ob sich die einzelne Lehrkraft über ausdrückliche Weisungen der Schulleitung hinweggesetzt hat und auf diese Weise selbst die Verantwortung für den Einsatz eines unzulässigen Verfahrens im Distanzunterricht trägt. Da keine schulgesetzliche Bestimmung die Schülerinnen und Schüler zum Einsatz von digitalen Lehr- und Lernmitteln verpflichtet, mit denen personenbezogene Daten verarbeitet werden, dürfen diese erst nach ausdrücklicher informierter (!) Einwilligung der Erziehungsberechtigten beziehungsweise der volljährigen Schülerinnen und Schüler eingesetzt werden: https://www.tlfdi.de/mam/tlfdi/datenschutz/anwendungsbeispiel_einwilligung_.pdf. Hierbei kann die Einwilligung jedoch nur die fehlende Rechtsgrundlage ersetzen, nicht aber zum Beispiel Verstöße gegen die Datensicherheit quasi „legalisieren“. Darüber hinaus muss mit der Stelle, die die Software anbietet, nach

Art. 28 DS-GVO ein Auftragsverarbeitungsvertrag abgeschlossen werden. Formulierungshilfen hierzu sind zu finden unter: https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungs-hilfe_fur_auftragsverarbeitungsvertraege.pdf. Die Beauftragung von US-Anbietern birgt die Gefahr, dass aufgrund der US-amerikanischen Rechtsvorschriften Zugriffe durch US-Stellen bestehen, die nach den europäischen Datenschutzbestimmungen nicht erlaubt sind. Der Einsatz dieser Produkte ist daher keinesfalls empfehlenswert. Auch auf die vom Thüringer Ministerium für Bildung, Jugend und Sport unter Mitarbeit des TLfDI herausgegebene Publikation „Antworten auf häufig gestellte Fragen zum Datenschutz in Schulen, Erfurt 2019“ wird unter Punkt 7.5 ausgeführt, dass Cloud-Angebote nichteuropäischer Anbieter für Unterrichtszwecke nicht genutzt werden dürfen: www.BildungTH.de/Datenschutz-in-Schulen. Dies hat der Europäische Gerichtshof in seinem Urteil vom 16. Juli 2020 (Rechtssache C 311/218 – „Schrems II“) ausdrücklich festgestellt. Personenbezogene Daten von Bürgern der EU dürfen nur in Drittländer übermittelt werden, wenn in dem Drittland ein vergleichbares Datenschutzniveau gegeben ist. Für die USA wurde dies ausdrücklich verneint (siehe Beitrag 2.1). Der TLfDI hat – neben weiteren Hinweisen auf seiner Homepage – darüber hinaus in den ersten drei Monaten des Jahres 2021 die Schulleitungen aller Thüringer Schulen in inzwischen vier Rundschreiben aus datenschutzrechtlicher Sicht über empfehlenswerte und nicht empfehlenswerte Schul-Apps, Online-Lernplattformen, Videokonferenzsysteme sowie Messenger-Dienste informiert (siehe Beitrag 3.16).
Stark nachgefragt sind auch die vom Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien organisierten Videokonferenzen mit Schulleitungen und dem TLfDI zu Fragen der Digitalisierung, die kontinuierlich fortgesetzt werden.

2.4 Corona-Warn-App

Für die Corona-Warn-App ist die zuständige datenschutzrechtliche Aufsichtsbehörde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Der TLfDI beobachtet aber weiterhin die Entwicklung der Corona-Warn-App, um unterstützend wirken zu können. Insbesondere wird der TLfDI den vorgeschriebenen Evaluierungsprozess und den vorgeschriebenen Prüfungsprozess nicht aus dem Blick verlieren.

Am 26. April 2020 informierte das Bundesgesundheitsministerium in einer Presseerklärung, dass, um Kontaktpersonen von Corona-Infizierten schnell und einfach warnen zu können, die Bundesregierung die Entwicklung einer Tracing-App beauftragt hat, deren Einsatz auf Freiwilligkeit beruht. Die App sei datenschutzkonform und solle ein hohes Maß an IT-Sicherheit gewährleisten. Am 16. Juni 2020 startete dann die „Corona-Warn-App".

Nach Kenntnisstand des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) basiert die App auf einem Kontakt-Erkennungs-Framework, welches im Frühjahr von Google und Apple vorgestellt wurde (siehe https://covid19.apple.com/contacttracing). Innerhalb dieses Frameworks werden nur Identifizierungswerte (Zufallszahlen) durch unterstützende Geräte ausgetauscht und auf den Geräten gespeichert. Erst bei einem Positivtest kann der Nutzer einer solchen App seine Zufallszahlen der letzten 14 Tage freigeben, welche durch die Server der App gesammelt und an alle Geräte verteilt werden. Diese Geräte prüfen dann innerhalb der App, ob Kontakt mit einem der Zufallszahlen bestand, wie lange der Kontakt dauerte und wie lange der Kontakt zurückliegt. Aus diesen Werten wird das individuelle Risiko jedes Einzelnen, sich infiziert zu haben, in der App berechnet und angezeigt. Mittlerweile gibt es eine neuere Version des Frameworks (siehe zum Beispiel https://developer.apple.com/documentation/exposurenotification/supporting_exposure_notifications_express und https://support.apple.com/de-de/HT209084#125), welche auch älteren Geräten die Nutzung der App ermöglichen soll. Hier gibt es zwar die Vorarbeit durch Google und Apple, allerdings ist die App auf diese Erweiterung noch nicht angepasst.

Die für diese App zuständige Datenschutzaufsichtsbehörde ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Der TLfDI beschäftigte sich trotzdem mit dem Thema, auch weil er teilweise zur App, zum technischen Verfahren und der Sicherheit angefragt wurde.

Für diese App wurde auch vom Verantwortlichen – der Bundesregierung – eine Datenschutz-Folgenabschätzung gemäß Art. 35 Datenschutz-Grundverordnung durchgeführt und im Internet veröffentlicht (https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf).

Der TLfDI wird die weitere Entwicklung der App und den Evaluierungsprozess sowie die entsprechende Prüfung weiter beobachten.

2.5 Thüringer Schulcloud

Die Thüringer Schulcloud wurde 2020 infolge der Corona-Pandemie wohl zum wichtigsten Werkzeug für den Distanzunterricht an Thüringer Schulen. Ihre Nutzung ist zwangsläufig mit der Verarbeitung einer Unmenge von personenbezogenen Daten verbunden. Der TLfDI hat die Entwicklung begleitet und wird gegebenenfalls auftretenden Datenschutzproblemen konsequent entgegentreten.

Wohl bei allen Schülergenerationen waren Hausaufgaben eher lästiges Übel. Da bringt es schon Abwechslung, wenn man dabei die Nase ins Internet statt ins Buch stecken kann. Auch wenn es sicher nicht Ziel des Thüringer Bildungsministeriums war, die Schülermeinung zu häuslichem Lernen zu ändern: Mit der Einführung der Thüringer Schulcloud (TSC) ist die Attraktivität beim Lernen sicher gewachsen und vor allem ist Lernen moderner geworden. Der TSC-Start für 20 Schulen war ein wichtiger Meilenstein in der „Digitalstrategie Thüringer Schulen“. Zeit wurde es. Mit Beginn der Corona-Pandemie bekam die TSC plötzlich einen viel höheren Stellenwert. Jetzt kam es für die Schulen praktisch drauf an, den gesamten Unterricht „auf Distanz“ zu managen. Die Thüringer Schulcloud (TSC) ist dabei wohl das wichtigste Digitalwerkzeug an mittlerweile 838 Thüringer Schulen geworden. Weitere Anträge liegen vor.
Von Anfang an war klar, dass bei der Nutzung solcher Werkzeuge eine Menge an personenbezogenen Daten von Schülerinnen, Schülern und Lehrkräften im Spiel sind. Da geht’s nicht nur um Anmeldedaten und IP-Adressen, sondern auch um Inhalte, die die Schüler in Aufsätzen, Präsentationen, Referaten und so weiter einstellen. Und in Videokonferenzen wandern Ton- und Bildaufnahmen durch das Netz. Nicht so gut für die Betroffenen, wenn das alles auf digitale Abwege geraten würde. Das hat natürlich den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf den Plan gerufen. Die TSC basiert auf einer Entwicklung des Hasso-Plattner-Instituts (HPI) in Potsdam und wird dort auch betrieben. Der TLfDI schaltete sich deshalb in seiner Rolle als Vorsitzender des Arbeitskreises der Datenschutzkonferenz „Schulen und Bildungseinrichtungen“ frühzeitig in die Entwicklung der HPI-Schulcloud ein. Das Ergebnis konnte danach als Landeslösung für Thüringen als Thüringer Schulcloud ohne Datenschutzbedenken übernommen werden.

Keine Bedenken heißt nicht, dass für alle Zeit alles in Ordnung sein muss. Funktionale und datenschutztechnische Schwachstellen zeigen sich häufig erst im Prozess. Das gilt für jede Software und das Risiko steigt mit ihrer Komplexität. Und fähige Leute – mit konstruktiver oder mit krimineller Absicht – werden versuchen, die Schwächen zu finden und auszunutzen. So auch bei der TSC, zu der entsprechende Berichte über Hacker-Angriffe in den Medien auftauchten. Die jeweiligen Lücken wurden beim HPI binnen weniger Stunden geschlossen. Die Vorfälle wurden vom Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien und HPI umgehend an den TLfDI gemeldet. Ein weiteres Eingreifen der Behörde war bislang nicht erforderlich. Das zeigt, dass Thüringen mit dem HPI auf den richtigen Partner gesetzt hat. Die Sache wird „rund“, wenn es gelingt, die Digitalisierung von Bildungsprozessen insgesamt so weit voran zu bringen, dass Videokonferenzen im Unterricht nicht regelmäßig wegen unzureichender Bandbreite im Fiasko enden und Lehrer wie Schüler auf ihre privaten Geräte angewiesen sind – Zeit wird’s.

2.6 Einigung in der DSK nicht immer einfach

Die DSK hat sich zum Ziel gesetzt, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen. Das ist angesichts ihrer föderalen Struktur und ihrer Unabhängigkeit nicht immer leicht. Dieses Gremium hat aber fundamentale Bedeutung, damit Deutschland auf europäischer Bühne mit einer Stimme sprechen kann. Dies ist nicht immer einfach, wie das Bespiel der datenschutzrechtlichen Bewertung von Microsoft-Produkten zeigt.

Die Datenschutzkonferenz (DSK) besteht aus den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten (vergleiche https://www.datenschutzkonferenz-online.de/dsk.html). Sie ist ein Gremium ohne eigene Rechtspersönlichkeit, hat aber gleichwohl eine wichtige Funktion. In den meisten anderen Ländern der Europäischen Union gibt es nur eine Datenschutzaufsichtsbehörde. Aufgrund der föderalen Struktur der Bundesrepublik Deutschland gibt es dort 18 Aufsichtsbehörden, zwei in Bayern, ansonsten eine in jedem Bundesland und den Bundesbeauftragten für

den Datenschutz und die Informationsfreiheit (BfDI). Jedes Land sowie der BfDI haben jeweils eine Stimme und treffen ihre Entscheidungen bis auf wenige Ausnahmen mehrheitlich. Dies namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. Weitere Einzelheiten können in der Geschäftsordnung der DSK nachgelesen werden (https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_geschaeftsordnung.pdf).
Da im Europäischen Datenschutzausschuss (EDSA) jeder Mitgliedstaat nur eine Stimme hat, wird in der DSK die deutsche Position für die Abstimmungen im EDSA gefunden. Außerdem ist sie bestrebt, in Deutschland eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts umzusetzen. Das ist nicht immer leicht, weil nach Art. 53 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist.
Dies zeigte sich auch bei der Bewertung von IT-Produkten der Firma Microsoft. Mit neun gegen acht Stimmen der DSK – also denkbar knapp – wurde beschlossen, dass die Bewertung seines Arbeitskreises Verwaltung zur Auftragsverarbeitung bei Microsoft Office 365 vom 15. Juli 2020 zustimmend zur Kenntnis genommen wird, so zu finden im Protokoll der entsprechenden Sitzung (https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf). Die Bewertung findet sich als Anlage zum Protokoll unter dem angegebenen Link. Sechs Aufsichtsbehörden (Baden-Württemberg, Bayern, Hessen, Rheinland-Pfalz, Saarland und Sachsen) hatten gebeten, ihr abweichendes Votum kenntlich zu machen. Aufgrund des, wenn auch knappen, Mehrheitsvotums wurden sowohl die Festlegung als auch die Bewertung öffentlich gemacht.
Die Landesbeauftragten für den Datenschutz von Baden-Württemberg, Bayern, Hessen, dem Saarland und der Präsident des Bayerischen Landesamtes für Datenschutz äußerten sich zu ihrem abweichenden Votum in einer gemeinsamen Presseerklärung (vergleiche https://www.lda.bayern.de/media/pm/20201002_office365.pdf).
Die DSK bat eine Arbeitsgruppe, auf Grundlage dieser Bewertungen Gespräche mit dem Hersteller aufzunehmen, um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des Europäischen Gerichtshofs (EuGH) aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen. Auch einige

Aufsichtsbehörden blieben nicht untätig. So äußerten sich die Aufsichtsbehörden der Länder Baden-Württemberg, Bayern und Hessen in miteinander abgestimmten Pressemitteilungen positiv über die Vorschläge, die Microsoft als einer der zentralen Anbieter global vernetzter IT-Produkte für Unternehmen für Garantien gemacht hat, die unmittelbar die Nutzerrechte stärken (vergleiche https://datenschutz.hessen.de/pressemitteilungen/microsoft-erg%C3%A4nzt-standardvertragsklauseln; https://lda.bayern.de/media/pm/pm2020_9.pdf; https://www.baden-wuerttemberg.datenschutz.de/dsgvowirkt/).
Die neuen Vertragsklauseln von Microsoft enthielten Regelungen über

- den Anspruch auf Schadensersatz für die betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat;
- die Information der betroffenen Person, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben;
- die Verpflichtung von Microsoft, den Rechtsweg zu beschreiten und die US-Gerichte anzurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten.

Damit sei, so die gemeinsame Bewertung der beteiligten Datenschutzaufsichtsbehörden, aber die Transferproblematik in die USA nicht generell gelöst – denn eine Ergänzung der Standardvertragsklauseln könne eben nicht dazu führen, dass der vom EuGH als unverhältnismäßig beanstandete Zugriff der US-amerikanischen Geheimdienste auf die Daten unterbunden werde.
Die Bewertung dieser Vorschläge durch den Arbeitskreis der DSK bleibt noch abzuwarten. Der Einsatz von US-Amerikanischen Produkten muss auch vor dem Hintergrund der Schrems II-Entscheidung des EuGHs (siehe Beitrag 2.1) gesehen werden. Er hat den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt. Damit ist die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield unzulässig. Die DSK hat zur Frage der Umsetzung des Urteils eine Task Force „Schrems II" eingerichtet, in der auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Mitglied ist (vergleiche https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf).

2.7 Windows 10

Die datenschutzgerechte Konfiguration von Windows 10 ist nach wie vor ein Problemthema – insbesondere die Telemetrieübertragung hat sich dabei als schwer deaktivierbar erwiesen. Für die „Enterprise“ Variante gibt es bereits Werkzeuge seitens Microsoft zur Einschränkung der Datenübermittlung. Für die „Home“ und „Professional“-Edition von Windows 10 sind praktisch immer tiefgreifende Systemmanipulationen durch externe Firewalls oder manuelle Manipulationen am System notwendig.

Windows 10 wird von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) seit dem Produktstart 2015 kritisch hinterfragt. So berichtete auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in seinem letzten Tätigkeitsbericht unter Nummer 2.11 über den aktuellen Stand zu Windows 10.
Es war erklärtes Ziel von Microsoft, sein Betriebssystem um Cloud-Funktionalitäten zu erweitern und die Betriebssystemdienste besser zu vernetzen. So werden durch das Betriebssystem Server von Microsoft angesprochen, welche zur Bereitstellung von Suchdiensten, Spracherkennung und Cloud-Speicher dienen. Aber auch Daten des Betriebssystems zum Betrieb (die sogenannte Telemetrie) und zum Beispiel Absturzberichte werden durch diese Server von Microsoft gesammelt. Für die Version 1909 kann man eine Liste dieser Server unter https://docs.microsoft.com/de-de/windows/privacy/windows-endpoints-1909-non-enterprise-editions finden, woraus hervorgeht, dass jede Windows 10-Version circa 50 dieser Server anspricht. Die Menge der Server ist also recht groß und Informationen, welche Datenverarbeitung auf diesen Servern eigentlich stattfindet, sind in der Datenschutzerklärung zu Windows 10 unter https://privacy.microsoft.com/de-de/privacystatement zu finden.
Aufgrund der hohen Verbreitung des Betriebssystems und der komplexen Datenverarbeitung seitens Microsoft auf deren Servern, hat die DSK am 26. November 2020 einen Beschluss „Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise“ veröffentlicht (zu finden unter https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf). Dabei hat die DSK die „Enterprise“ Version von Windows 10 in Bezug auf die Telemetrie betrachtet. Dies ist nur ein

kleiner Teil der Datenübertragung zu Microsoft, gehört aber zu den komplexeren Übertragungsmechanismen, welche es Programmierern erlauben, fast beliebige Datenströme in zentralen Betriebssystemkomponenten zu erfassen und an Microsoft zu übertragen. Der Inhalt der Telemetrie ist sehr frei gestaltbar. Das Übertragungsziel der Telemetrie betrifft die Endpunkte „*.blob.core.windows.net“, „watson.telemetry.microsoft.com*“ und „settings-win.data.microsoft.com“.
In den Tests der DSK wurden verschiedene Szenarien umgesetzt, vom Betriebssystem mit Standardeinstellungen über ein System, bei welchem das Telemetrie-Level per Gruppenrichtlinie auf das Level „Security“ beschränkt wurde, bis zu einem System, welches mit dem Telemetrie-Level „Security“ arbeitet und zusätzlich die „Windows Restricted Traffic Limited Functionality Baseline“ nutzt (zu finden unter https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services). Sowohl die Baseline als auch die Einstellung für das Telemetrie-Level „Security“ sind ausschließlich für Windows 10 Systeme mit „Enterprise“ Lizenz verfügbar. In den Systemen Windows 10 „Professional“ oder „Home“ Lizenz kann man diese Einstellungen momentan nicht vornehmen. In den Tests haben sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch die Landesdatenschutzbeauftrage Niedersachsens herausgefunden, dass dennoch Datenverbindungen (sporadisch) zu settings-win.data.microsoft.com aufgebaut werden.
Unglücklicherweise konnte weder Microsoft den Datenschutzaufsichtsbehörden mitteilen, welche Daten über den Kanal gesendet werden, noch konnten diese aufgrund der eingesetzten Verschlüsselung die Daten einsehen. So ist bis heute unklar, welche Daten (trotz der maximalen Systemeinschränkung) noch zu Microsoft gesendet werden. Wie das BSI in seiner SySiPhus-Studie zu den Telemetriekomponenten herausfand, ist der Endpunkt settings-win.data.microsoft.com ein Teil der Telemetrieinfrastruktur (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html, Version 1.2, Anhang Seite 25). Somit gibt es nach Auffassung des TLfDI bisher keinen Weg, mit Boardmitteln von Windows 10 die Telemtriedaten komplett zu deaktivieren. Ob öffentliche Stellen diese Daten aber an Microsoft senden dürfen, ist anzuzweifeln.
Im oben erwähnten Beschluss der DSK wird ausdrücklich festgestellt, dass es keinesfalls ausreichend ist, mit Telemetrie-Level „Security“

die Enterprise-Version von Windows 10 datenschutzgerecht einzustellen. Vielmehr muss der Verantwortliche auch klären, dass keine Daten an Microsoft gesendet werden, für welche der Verantwortliche keine Rechtsgrundlage zur Verarbeitung besitzt. Daher empfiehlt der TLfDI insbesondere für öffentliche Stellen zusätzlich den Einsatz der „Windows Restricted Traffic Limited Functionality Baseline“ und das Blocken von Verbindungen zu „settings-win.data.microsoft.com“. Damit sind sehr viele vernetzte Betriebssystemdienste deaktiviert und auch die Telemetrieübertragung wird wirksam unterbunden. Da Microsoft die Telemetriekonfiguration und den Systemaufbau mit zukünftigen Updates jederzeit ändern kann, muss die Wirksamkeit der Maßnahmen regelmäßig überprüft werden. Für Windows 10 „Professional“ und „Home“ gibt es allerdings die beschriebenen Maßnahmen nicht. Hier muss das System aufwändig manuell angepasst werden, wie dies unter anderem in der SySiPhus Studie (siehe Link oben) näher in den Abschnitten 3.1.2, 3.1.4, 3.1.5 und 3.2 beschrieben wird.
Da die datenschutzgerechte Konfiguration von Windows 10 momentan sehr aufwändig ist, hat die DSK in ihrem Beschluss Microsoft daher aufgefordert, einfache Konfigurationsmöglichkeiten für alle Windows 10-Varianten anzubieten.

2.8 Digitale Souveränität

Die DSK ist zu Recht der Ansicht, dass die Stärkung der Digitalen Souveränität in der öffentlichen Verwaltung große strategische Bedeutung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in ihrer Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

Die Konferenz der IT-Beauftragten der Bundesressorts (KoITB) veröffentlichte im Januar 2020 den Beschluss „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung, Eckpunkte – Ziel und Handlungsfelder“. In diesem Beschluss wird die digitale Souveränität definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Eine solche Ausübung ist insbesondere für die Öffentliche Verwaltung zur Erfüllung ihrer ho-

heitlichen Aufgaben durch digitale Verwaltungsprozesse wichtig“. Nach Angaben der KoITB identifizierte aber eine entsprechende Marktanalyse durch Abhängigkeiten verursachte kritische Schmerzpunkte, insbesondere in der Informationssicherheit und bei der Gewährleistung datenschutzrechtlicher Vorgaben, welche die Selbstständigkeit, Selbstbestimmung und Sicherheit der Öffentlichen Verwaltung in der digitalen Welt beeinträchtigen können.
Die KoITB bat den IT-Planungsrat, den gefassten Beschluss der KoITB zu bestätigen. Im März 2020 veröffentlichte der IT-Planungsrat einen entsprechenden Beschluss.
Dies nahm wiederum die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zum Anlass, sich aus ihrer Sicht zu dem Thema zu positionieren und veröffentlichte im September 2020 eine Entschließung „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen“. In dieser Entschließung teilt sie die Einschätzung des IT-Planungsrats, dass die digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist, da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich.
Die DSK sieht deren Gewährleistung aber als ein vordringliches Handlungsfeld an. Konkret fordert die DSK den Bund, die Länder und die Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,
- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und
- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Eine der von der DSK dann aufgeführten fünf kurzfristig umzusetzenden Maßnahmen dabei sind die Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung

von Prozessen. Dies bedeutet: Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 Datenschutz-Grundverordnung erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche in der öffentlichen Verwaltung sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.
Die vollständige Entschließung der DSK finden Sie unter: https://www.datenschutzkonferenz-online.de/entschliessungen.html.

2.9 Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen

Aus der DS-GVO ergeben sich umfangreiche Anforderungen zur Einhaltung datenschutzrechtlicher Grundsätze im Zusammenhang mit der IT-Infrastruktur. Daneben haben die Verantwortlichen ergänzende Anforderungen aus der Bundes- sowie Landesgesetzgebung zwingend zu prüfen und vollständig in ihre Verwaltungsabläufe einzubeziehen.

In Art. 5 der Datenschutz-Grundverordnung (DS-GVO) sind die Grundsätze der Verarbeitung personenbezogener Daten geregelt. So sind gemäß Art. 5 Abs. 1 DS-GVO die Rechtmäßigkeit, die Verarbeitung nach Treu und Glauben, die Transparenz, die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung und die Integrität und Vertraulichkeit zu gewährleisten. Dabei ist der Verantwortliche für die Einhaltung dieser Grundsätze verantwortlich und muss dessen Einhaltung auch nachweisen können („Rechenschafts-

pflicht“, Art. 5 Abs. 2 DS-GVO). Gemäß Art. 32 Abs. 1 DS-GVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden (Art. 32 Abs. 2 DS-GVO). Diese Maßnahmen schließen gegebenenfalls auch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein (Art. 32 Abs. 1 Buchstabe d) DS-GVO). Mit dem Standard-Datenschutzmodell (SDM) stellt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein Werkzeug bereit, mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird, siehe hierzu auch Beitrag 2.13. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat Hinweise zu „Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen“ veröffentlicht. Die Hinweise richten sich dabei an die Verantwortlichen und entsprechenden Auftragsverarbeiter. So wird das SDM erläutert und eine Checkliste bereitgestellt, um die getroffenen Mindestanforderungen zu überprüfen. Die Hinweise des TLfDI sind abrufbar unter: https://tlfdi.de/mam/tlfdi/datenschutz/ds-anforderungen-it-sicherheit_offtl_stellen_stand_februar_2021.pdf.

2.10 E-Mailverschlüsselung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Orientierungshilfe zu „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ veröffentlicht. Es wird beschrieben, was beim Empfang

und Versenden von E-Mails sowohl bei „normalem Risiko“ und „hohem Risiko“ beachtet werden muss. Dabei spielen die Transportverschlüsselung und die Ende-zu-Ende-Verschlüsselung eine wesentliche Rolle, um die Sicherheit des Inhalts zu gewährleisten.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich 2020 mit dem Thema „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ beschäftigt und im März 2020 eine entsprechende Orientierungshilfe veröffentlicht (siehe https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf).
Die Orientierungshilfe geht von typischen Verarbeitungssituationen aus. Sie bestimmt hierbei ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail die Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung der Risiken zu treffen haben. Verantwortliche und Auftragsverarbeiter sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Die Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit (das heißt, Dritte könnten den Inhalt mitlesen) und Integrität (das heißt, Dritte könnten den Inhalt manipulieren) personenbezogener Daten verbunden sind. Sie setzt voraus, dass die Verantwortlichen beziehungsweise ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können. Für die Risikoabschätzung sei an dieser Stelle auf das Kurzpapier Nr. 18 der DSK verwiesen (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). Die aus der Risikoeinschätzung resultierende Risikostufe („normales Risiko“ oder „hohes Risiko“) ist maßgeblich für die zu treffenden Maßnahmen.
Neben grundlegenden Anforderungen an die Auswahl der Anbieter und ebenso grundlegende Sicherheitsanforderungen an die Server (Kapitel 3 der Orientierungshilfe), werden in Kapitel 4 Anforderungen je nach Risikostufe gestellt. Dabei geht die Orientierungshilfe davon aus, dass bei der Datenübertragung von Daten mit „normalem Ri-

siko“ eine Transportverschlüsselung nach dem Stand der Technik ausreichend ist. Werden Daten mit „hohem Risiko“ versendet oder empfangen, muss zusätzlich eine Ende-zu-Ende-Verschlüsselung eingesetzt werden, optional kann für die Transportverschlüsselung zusätzlich ein qualifiziertes Server-Zertifikat genutzt werden, um die Authentizität/ Echtheit der beteiligten Server zu überprüfen. Die Ende-zu-Ende-Verschlüsselung ermöglicht außerdem die Signierung der Mail, um die Echtheit des Senders prüfen zu können. Der Einsatz von Transportverschlüsselung bietet einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht. Die Transportverschlüsselung reduziert jedoch lediglich die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Zudem prüfen die beteiligten Provider in der Regel nach Eingang einer Nachricht diese unmittelbar auf Schadsoftware. Dies bedeutet, dass dort jede Mail für einen kurzen Moment automatisch geprüft wird, bevor sie weitergeleitet oder für den Abruf gespeichert wird. Durch eine Ende-zu-Ende-Verschlüsselung ist es hingegen möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern.
Wie aber realisiert man eine Transportverschlüsselung beziehungsweise Ende-zu-Ende-Verschlüsselung? Die Transportverschlüsselung wird im Großteil der Fälle bereits ohne Zutun des Nutzers verwendet und ist ein etablierter technischer Standard. Nutzt man sein E-Mail-Postfach über den Browser, erscheint zum Beispiel ein Schlosssymbol in der Adressleiste oder das Kürzel https:// vor der Web-Adresse. In diesem Fall werden die Daten über das verschlüsselte Webprotokoll HTTPS zum E-Mail-Server übertragen. Nutzt man eigenständige E-Mail-Clients, wie zum Beispiel Outlook, Thunderbird oder Apple-Mail, so erfolgt die Konfiguration der Verschlüsselung (meist unbewusst) bei der Einbindung des Postfachs in den Client. Tauchen in der Konfiguration für den Mailempfang (Protokolle IMAP oder Pop3) beziehungsweise den Mailversand (Protokoll SMTP) Begriffe wie „TLS“, „STARTTLS“ oder „Verschlüsselung“ auf, wird eine Transportverschlüsselung genutzt. Im Zweifel sollte man hier seinen Anbieter kontaktieren.

Für eine Ende-zu-Ende-Verschlüsselung ist eine Zusatzsoftware notwendig, welche entweder beim E-Mail-Client dazu installiert werden oder per Browser-Plug-In eingebunden werden muss. Weiterhin müssen Sender und Empfänger vor Anwendung der Verschlüsselung ihre öffentlichen Schlüssel austauschen, was manchmal noch manuell erfolgen muss, oder auch teilweise automatisiert erfolgt. Entsprechend der Orientierungshilfe ist es durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen.
Weitere Informationen zu dem Thema hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht, siehe hierzu zum Beispiel https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/email_verschluesselung_node.html und https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_in_der_Praxis_node.html.

2.11 Datenschutz-Folgenabschätzung (DS-FA) für den öffentlichen Bereich

Die nach Art. 35 DS-GVO durchzuführende Datenschutz-Folgenabschätzung (DS-FA) beruht auf dem risikobasierten Ansatz. Der TLfDI hat in Bezug auf die Notwendigkeit einer DS-FA und deren praktische Umsetzung eine Handreichung zur DS-FA für den öffentlichen Bereich erstellt.

Mit der Datenschutz-Folgenabschätzung (DS-FA) verpflichtet die Datenschutz-Grundverordnung (DS-GVO) in Art. 35 Abs. 1 DS-GVO den Verantwortlichen vor einer Verarbeitung von personenbezogenen Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte in seinem Tätigkeitsbericht für den Berichtszeitraum 2019, dass er hierzu eine Handreichung für den nicht-öffentlichen Bereich veröffentlicht hat. Nunmehr liegt auch eine angepasste Handreichung für den öffentlichen Bereich vor. Ziel ist da-

bei, den Landes- und Kommunalbehörden eine diesbezügliche Hilfestellung zu geben.
Wie schon im letzten Tätigkeitsbericht dargestellt, ist eine DS-FA ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Durch den technikneutralen Ansatz des sachlichen Anwendungsbereiches der DS-GVO ist es ohne Belang, ob es sich um ein automatisiertes Verfahren oder um eine nicht-automatisierte Verarbeitung, zum Beispiel von Personaldaten in Papierakten, handelt. Dabei ist zu beachten, dass die DS-FA kein einmaliger Vorgang ist. Wenn Risiken hinzutreten oder sich Verarbeitungsvorgänge oder auch der Stand der Technik grundlegend ändern, muss erneut eine DS-FA durchgeführt werden. Somit wiederholt sich der Prozess der Datenschutz-Folgenabschätzung zyklisch und ermöglicht auf diese Weise eine kontinuierliche Überprüfung und gegebenenfalls die Anpassung der Verarbeitung personenbezogener Daten. Die formellen Anforderungen an eine DS-FA sind in Art. 35 DS-GVO geregelt. Weiterhin finden sich Hinweise in den Erwägungsgründen 84 und 89 bis 93 der DS-GVO. Die Methodik der Durchführung wird in der DS-GVO nicht festgelegt. Hier besteht ein gewisser Spielraum für die Verantwortlichen. Es ist jedoch ratsam, auf bestehende Methoden oder Standards zurückzugreifen. Ein Beispiel ist die Methodik nach dem Standard-Datenschutzmodell (SDM) in seiner jeweiligen aktuellen Version, siehe Beitrag 2.13. Bevor eine DS-FA durchgeführt wird, ist in einem ersten Schritt zu klären, ob überhaupt eine Notwendigkeit zur Durchführung besteht, das heißt, ob überhaupt die Verarbeitung vorgesehen ist, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.
Die Handreichung gibt dem Verantwortlichen ein Prüfungsschema an die Hand, mit welchem er prüfen kann, ob eine Notwendigkeit zur Durchführung einer DS-FA besteht. Auch wird darauf eingegangen, wer diese Vorprüfung durchführt. Kommt der Verantwortliche in der Vorprüfung zu dem Ergebnis, das eine DS-FA durchzuführen ist, gibt die Handreichung Hilfestellung bei der Durchführung der DS-FA. Dazu wird dargestellt, wer die DS-FA durchführt, welchen Umfang eine DS-FA hat und welche Schritte bei der Durchführung zu befolgen sind. Dabei werden insbesondere im Abschnitt Maßnahmen konkrete Beispiele und weiterführende Informationen zu technischen und organisatorischen Maßnahmen benannt. Auch die erstellten komprimierten grafischen Übersichten der Vorprüfung sowie des Gesamtprozes-

ses der DS-FA sollen den Verantwortlichen durch die DS-FA lotsen. Die Handreichung des TLfDI finden Sie unter: https://tlfdi.de/mam/tlfdi/datenschutz/handreichung_zur_datenschutz-folgenabschatzung.pdf.

2.12 Videokonferenzsysteme

Auch bei der Nutzung von Videokonferenzsystemen werden personenbezogene Daten verarbeitet, sodass die DS-GVO auch bei solchen Systemen eingehalten werden muss. Die DSK hat dazu eine Orientierungshilfe und eine Checkliste veröffentlicht.

Die Nutzung von Videokonferenzsystemen datenschutzrechtlich zulässig zu gestalten, ist derzeit ein aktuelles Thema. Schließlich können inhaltliche Äußerungen und die Übertragung von Ton und Bild der teilnehmenden Personen und gegebenenfalls ihres Umfeldes, wie etwa ihrer Wohnung, ihres Arbeitsplatzes oder sonstigen Aufenthaltsorts (Inhaltsdaten) betroffen sein. Bild- und Tonaufnahmen der Teilnehmenden enthalten auch genügend Informationen, um diese anhand ihrer Stimme oder ihrer Gesichtsmerkmale identifizieren zu können. Je nach Art des Dienstes sind aber daneben auch Äußerungen in Form von grafischen oder textlichen Chatnachrichten oder die Anzeige des eigenen Bildschirms für einzelne oder alle Teilnehmer möglich; die Zuordnung dieser Nachrichten oder Anzeigevorgänge zu den teilnehmenden Personen, die sie geäußert, präsentiert oder rezipiert haben, ist dabei auch als personenbezogen zu betrachten. Zudem können auch personenbezogene Daten von Personen aus dem Umfeld der teilnehmenden Personen betroffen sein, deren Bild oder Ton unter Umständen von dem Konferenzsystem mitverarbeitet werden. Beispiel: eine Person aus dem Haushalt des Konferenzteilnehmers läuft durch das Bild oder spricht im Hintergrund. Zusätzlich starten viele Videokonferenzsysteme ihre Konferenzen über ein Webportal. In diesem Portal können zusätzlich Tracking-, Werbe- und Marketingwerkzeuge integriert sein, so dass bei der Nutzung weitere Nutzerinformationen erhoben werden, die über Bild und Ton hinausgehen. Hier gibt es die Gefahr, dass die anfallenden Metadaten mit anderen Daten kombiniert werden können (zum Beispiel durch Dienste wie Google-Analytics) und zur Erstellung von Nutzerprofilen beitragen, die auch gegen den Nutzer verwendet werden könnten. Deshalb hat die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und

der Länder (DSK) am 23. Oktober 2020 eine „Orientierungshilfe Videokonferenzsysteme“ veröffentlicht und am 11. November 2020 zusätzlich auch noch eine entsprechende Checkliste zur Verfügung gestellt, in der dargelegt wird, welche Anforderungen an den datenschutzkonformen Betrieb von Videokonferenzsystemen zu stellen sind.

Durch das Urteil des Europäischen Gerichtshofes „Schrems II“, Aktenzeichen C-311/18, wurde die Vereinbarung zum „privacy shield“ für ungültig erklärt, da die USA kein der EU vergleichbares Datenschutzniveau bieten. Eine Datenübermittlung in die USA ist – sofern überhaupt – nur unter den sehr engen Bedingungen dieses Urteils möglich.

Die vorliegende Orientierungshilfe erläutert datenschutzrechtliche Anforderungen an die Durchführung von Videokonferenzen durch Unternehmen, Behörden und andere Organisationen. Der Verantwortliche hat grundsätzlich drei Möglichkeiten, ein Videokonferenzsystem zu betreiben: Entweder betreibt er das System selbst oder lässt das System bei einem externen IT-Dienstleister betreiben oder nutzt einen Online-Dienst (Software as a Service). Die Orientierungshilfe legt für diese drei Betriebsmodelle die rechtlichen Anforderungen sowie die technischen und organisatorischen Anforderungen dar.

So weist sie zum Beispiel darauf hin, dass der für die Durchführung der Videokonferenz Verantwortliche verpflichtet ist, zu prüfen, inwieweit er zur Verarbeitung überhaupt befugt ist. Außerdem ist das Videokonferenzsystem gemäß Art. 24, 25 und 32 Datenschutz-Grundverordnung (DS-GVO) durch die Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen so einzurichten, dass es den Anforderungen der DS-GVO an die Verarbeitung personenbezogener Daten genügt.

Videokonferenzsysteme müssen beispielsweise eine Verschlüsselung nach dem Stand der Technik implementieren. Hierzu liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zu geeigneten kryptographischen Verfahren.

Für die Übertragung von Videokonferenzdaten ist mindestens eine Transportverschlüsselung entsprechend den einschlägigen technischen Richtlinien des BSI erforderlich. Die Transportverschlüsselung muss die Vertraulichkeit, Integrität und Authentizität aller übertragenen Daten gewährleisten: der Inhaltsdaten wie auch der Rahmendaten.

Insbesondere wenn die Verarbeitung von Daten im Rahmen einer Videokonferenz zu einem hohen Risiko für betroffene Personen führen

kann, müssen der Verantwortliche und gegebenenfalls der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um die Vertraulichkeit der übermittelten Inhaltsdaten auf zentralen Servern und den anderweitig beteiligten IT-Komponenten sicherzustellen. Dies ist zum Beispiel dann der Fall, wenn Gesundheitsdaten in Videokonferenzen besprochen werden (zum Beispiel bei digitalen Sprechstunden, Terminen bei Suchtberatungsstellen oder Schwangerschaftskonfliktberatungen und so weiter) oder in denen Informationen zum Sozialstatus besprochen werden (Schuldnerberatung, Zwangsversteigerungstermine, Termine Langzeitarbeitsloser bei der Arbeitsagentur) oder bei sensiblen Daten aus dem Schulbereich. Bei solch sensiblen Daten sollte die Vertraulichkeit beispielsweise über eine Ende-zu-Ende-Verschlüsselung und eine Verschlüsselung gespeicherter Daten sichergestellt werden. Bei einer Ende-zu-Ende-Verschlüsselung können nur Sender und Empfänger die Daten entschlüsseln – alle an der Übertragung beteiligten Server können dies nicht. Bei der Transportverschlüsselung kann mindestens ein weiterleitender Server die Daten entschlüsseln. Eine wirksame Ende-zu-Ende-Verschlüsselung setzt dabei voraus, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentisieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt beziehungsweise verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist. Weiterhin hat der Verantwortliche auch insbesondere den Grundsatz der Datensparsamkeit zu beachten. Deshalb muss er prüfen, inwieweit die mit dem konkreten Einsatz des Konferenzsystems verbundene Datenverarbeitung auf das zur Zweckerreichung Erforderliche begrenzt werden kann. Ferner hat er über die Datenverarbeitung in der gebotenen Form zu informieren.
Soweit der Verantwortliche Tools eines Anbieters verwendet, muss er auch die datenschutzrechtliche Beziehung zum Anbieter klären und gegebenenfalls einen Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO abschließen. Er hat auch dann darauf zu achten, dass die zum Schutz der jeweiligen Daten erforderlichen technischen und organisatorischen Maßnahmen ergriffen werden.
Die Orientierungshilfe der DSK und die Checkliste sollen den Verantwortlichen eine Hilfestellung bieten, um für seinen jeweiligen Einzelfall die jeweils notwendige Videokonferenz aus datenschutzrechtlichen Gesichtspunkten auszuwählen und sicherer zu gestalten. Sowohl die Orientierungshilfe als auch die Checkliste sind abrufbar unter

https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

2.13 Das Standard-Datenschutzmodell (SDM) – Version 2.0b

Das Standard-Datenschutzmodell wurde von der DSK erarbeitet und war bereits 2018 unter Nummer 5.26 Gegenstand des 1. Tätigkeitsberichts zum Datenschutz nach der DS-GVO. Seit April 2020 liegt die überarbeitete Version 2.0b vor. Zudem wurden bisher diesbezüglich sieben verbindliche Bausteine mit dem Zweck der praktischen Nutzung veröffentlicht.

Im April 2020 beschloss die 99. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) das „Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“ (SDM), Version 2.0b. Darin werden rechtliche Anforderungen der Datenschutz-Grundverordnung (DS-GVO) vollständig erfasst und systematisiert durch Gewährleistungsziele untersetzt. Mit dem SDM stellt die Konferenz ein Werkzeug bereit, mit dem die von der DS-GVO geforderten technischen und organisatorischen Maßnahmen rechtskonform abgeleitet werden können.
Derzeit gibt es sieben veröffentlichte Bausteine, die an dieser Stelle kurz charakterisiert werden. Es handelt es sich um die Bausteine „Aufbewahren“, „Dokumentieren“, „Protokollieren“, „Trennen“, „Löschen und Vernichten“, „Berichtigen“ und „Einschränken der Verarbeitung“.
Der Baustein „Aufbewahren“ beschreibt diejenigen Maßnahmen zur Verarbeitung von personenbezogenen Daten, die zum Aufbewahren in physikalischen Speichermedien/ Datenträgern über längere Zeiträume im Sinne eines Langzeitspeichersystems erforderlich sind, um auf sie während des gesamten Aufbewahrungszeitraums zugreifen zu können. Der Begriff des Aufbewahrens wird hier für die langfristige Informationserhaltung von Datenobjekten mit Personenbezug verwendet.
Der Baustein „Dokumentieren“ beschreibt die Verarbeitung unter Ausweis des Zwecks der Verarbeitungstätigkeit und der Zweckbindung der verarbeiteten Daten. Das Dokumentieren dient dazu, die rechtmäßige Verarbeitung dauerhaft sicherzustellen und nachzuweisen. Es unterstützt den Verantwortlichen und gegebenenfalls den Auf-

tragsverarbeiter bei der Erfüllung der Informationspflichten sowie der Gewährleistung der Auskunftsrechte gegenüber der betroffenen Person.
Der Baustein „Protokollieren“ beschreibt Möglichkeiten, in der Vergangenheit liegende Verarbeitungen prüfbar zu machen. Die Prüfbarkeit ist eine notwendige Voraussetzung für den Nachweis einer wirksamen Umsetzung der gesetzlichen Anforderungen und deren Beurteilung im Sinne der Rechenschaftspflicht des Verantwortlichen und gegebenenfalls des Auftragsverarbeiters.
Der Baustein „Trennen“ listet Prüfschritte und Maßnahmen auf, mit denen Trennungsanforderungen an Daten, Systeme und Dienste sowie Prozesse umgesetzt werden können. Dies betrifft sowohl die Trennung innerhalb einer Organisation als auch von miteinander zusammenarbeitenden Organisationen. Eine Trennung ist eine Voraussetzung dafür, rechtlich zulässige Verbindungen zwischen verschiedenen Organisationen (und selbstständigen Organisationseinheiten) mit deren Daten, Systemen und Diensten sowie Prozessen unter organisatorischen und technischen Bedingungen herstellen zu können.
Der Baustein „Löschen und Vernichten“ beschreibt die Facetten, die in Abhängigkeit vom Risiko, das aus der Verarbeitung der betreffenden Daten für die betroffene Person resultiert, zu berücksichtigen sind. Die technischen und organisatorischen Maßnahmen zum Löschen und Vernichten müssen dem Schutzbedarf der betroffenen natürlichen Personen und somit dem Risiko, das aus der Verarbeitung der betreffenden Daten resultiert, angemessen sein. Es kommen daher verschiedene Methoden für das Löschen und Vernichten in Betracht, die in einer Liste mit abgestufter Aufzählung erläutert werden. In der Reihenfolge dieser Liste nimmt der Aufwand für die Rekonstruierung von personenbezogenen Daten zu.
Der Baustein „Berichtigen“ beschreibt Verfahren, die Verantwortliche und gegebenenfalls Auftragsverarbeiter anwenden müssen, wenn verarbeitete Daten unrichtig oder aber nicht auf dem neuesten Stand sind. Dies betrifft zum einen den Grundsatz der Datenrichtigkeit und zum anderen das Recht der betroffenen Person zur Berichtigung ihrer verarbeiteten Daten. Erkannte beziehungsweise angezeigte Berichtigungserfordernisse sind unverzüglich umzusetzen.
Der Baustein „Einschränken der Verarbeitung“ schließlich unterstützt dabei, dass nach einer entsprechenden Entscheidung des Verantwortlichen beziehungsweise des Auftragsverarbeiters die von der Einschränkung betroffenen personenbezogenen Daten nicht mehr verar-

beitet werden können, obwohl sie auf den technischen Systemen noch vorgehalten werden (müssen).
Die aktuelle Version des SDM in der Version 2.0b mit den Bausteinen (Maßnahmenkatalog) ist unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ abrufbar.

2.14 Smart-City

Smart City ist eins der Schlagworte 2020 im kommunalen Bereich. Aus Sicht des TLfDI bedürfen alle Projekte weiterhin der vollen Aufmerksamkeit des Datenschutzes bei der Umsetzung gemäß der DS-GVO. Der TLfDI ist gerne bereit, solche Projekte datenschutzrechtlich beratend mit zu begleiten.

Seitens des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit wurde bereits 2017 eine „Smart City Charta – Digitale Transformation in den Kommunen nachhaltig gestalten“ veröffentlicht. Sie beinhaltet unter anderem entsprechende Leitlinien, Handlungsempfehlungen und Beispiele. So heißt es in der Charta: Die Smart City Charta richtet sich an Städte, Kreise und Gemeinden (Kommunen). Sie richtet sich ebenso an Akteure aus Forschung, Wirtschaft und Zivilgesellschaft. Die Smart City erweitert das Instrumentarium der nachhaltigen und integrierten Stadtentwicklung um technische Komponenten, sodass die Gesellschaft, der Mensch und seine Lebensgrundlagen auch zukünftig im Mittelpunkt stehen. Kommunen sollten frühzeitig die strategischen Handlungsfelder der Smart City für sich identifizieren und definieren. Schwerpunkte können zum Beispiel eine höhere Effizienz der Verwaltung, mehr Transparenz und Partizipation, das Erreichen konkreter Klimaziele, optimierte Mobilität und Verkehrsabläufe oder die regionale Innovations- und Wirtschaftsförderung sein.
Die Bundesregierung fördert dabei die digitale Modernisierung der Kommunen durch Smart-City-Modellprojekte. Auf Grundlage der „Smart City Charta“ sollen Städte und Gemeinden unterstützt werden. Im März 2020 veröffentlichte das Bundesministerium des Innern, für Bau und Heimat dazu ein Dokument „Technischer Leitfaden für Modellprojekte Smart Cities: Stadtentwicklung und Digitalisierung“. Dieser Leitfaden beinhaltet umfassende Informationen, wie sich Kommunen an einem entsprechenden Förderprogramm mit welchen Vorgaben bewerben können.

Nach Kenntnisstand des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Stand 31. Dezember 2020, nehmen aus Thüringen die Stadt Gera, die bereits seit 2019 Pilotkommune des Modellprojektes Smart Cities des Bundesministeriums des Inneren ist und auch die Stadt Jena am Modellprojekt des Förderprogramms teil. Es ist zu erwarten, dass weitere Thüringer Kommunen folgen werden.

Der TLfDI möchte dies zum Anlass nehmen, darauf hinzuweisen, dass, soweit personenbezogene Daten verarbeitet werden sollten, stets die Umsetzung der Datenschutz-Grundverordnung (DS-GVO) und auch die digitale Souveränität im Blick zu behalten sind. Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten (siehe Beitrag 2.8).

In jedem Fall sind vor der Einführung eines Verfahrens oder Projektes die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DS-GVO, die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO und die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO zu prüfen. Gegebenenfalls ist auch zuvor eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich.

Der TLfDI ist gerne bereit, solche Projekte datenschutzrechtlich beratend mit zu begleiten, erste Gespräche gab es schon mit der Stadt Gera. Aus Sicht des TLfDI sollten die Projekte zielgruppen- und altersorientiert datenschutzfreundlich gestaltet werden. So teilt der TLfDI die Meinung im „Achten Altersbericht der Bundesregierung“ (Bundestagsdrucksache 19/21650), dass Smart Cities nur realisiert werden können, wenn zum einen die technische Infrastruktur überall realisiert wird und zum anderen die Kommunen sich strategisch aufstellen und sich den digitalen Wandel zunutze machen, indem sie digitale Ange-

bote schaffen, die auch den unterschiedlichen Möglichkeiten der älteren Menschen Rechnung tragen. Dabei sind nicht nur die kostenfreie Internetnutzung im öffentlichen Raum und der Zugang zu Geräten und Software relevant, sondern auch die zielgruppenspezifische Unterstützung durch zum Beispiel Helferstrukturen oder Paten- und Netzwerke. Dem Bericht zufolge wird zudem im Zuge der Digitalisierung von Lebens- und Alltagswelten an ältere Menschen die gesteigerte Erwartung gestellt, mit diesen Technologien souverän interagieren zu können, um von ihrem Nutzen zu profitieren. Hier besteht – laut Bericht – die Gefahr, dass ältere Menschen mit der dynamischen Entwicklung der digitalen Technologien nicht mehr Schritt halten können und sich somit eine bereits heute erkennbare digitale Spaltung weiter verschärft. Deshalb muss das Ziel sein, auch für die zunehmende Zahl der älteren Menschen in Deutschland, in Zukunft die Teilhabe sicherzustellen und gleichwertige Lebensverhältnisse im Blick zu behalten oder zu fördern.

Aus Sicht des TLfDI beginnt dies schon bei barrierefreien Datenschutzerklärungen auf Webseiten und Apps und geht bis zur transparenten und nachvollziehbaren Gestaltung von Informationen zur Verarbeitung in Vorgängen und Projekten für die Nutzer. Auch ist zu beachten, dass die Einwilligungen zu diesen Verfahren oder Projekten nach Art. 7 Abs. 1 DS-GVO nur wirksam sind, wenn sie freiwillig abgegeben werden, das Kopplungsverbot eingehalten und sie in leichter Sprache sowie in informierter Art und Weise eingeholt wurden. Weiterhin unterliegt die wirksame Einwilligung der Zweckbindung und einem Widerrufsrecht. Auch müssen die Folgen der Verweigerung dargestellt werden.

Aus Sicht des TLfDI sind jedoch nicht nur die älteren Bürger bei der Gestaltung der digitalen Gesellschaft im Blick zu behalten. Der TLfDI, in seiner Eigenschaft als Vorsitzender zweier Arbeitskreise „Schulen und Bildungseinrichtungen“ sowie „Datenschutz-/ Medienkompetenz“, kämpft seit Jahren dafür, dass Lehrer und Schüler Medienkompetenz erlangen, damit sie in der jetzigen und zukünftigen digitalen Gesellschaft souverän und kompetent selbstbestimmend agieren können. Auch hier besteht die gesteigerte Erwartung, mit diesen Technologien zukünftig souverän interagieren zu können, um von ihrem Nutzen zu profitieren. Dies geht aber nur, wenn Medienkompetenz endlich zukünftig noch stärker in der Bildungspolitik verankert wird, wofür sich der TLfDI weiter einsetzen wird.

Nicht nur bei älteren Bürgern sollten in Zukunft die gleichwertigen Lebensverhältnisse im Blick behalten werden; jede Generation muss, entsprechend ihrer Lebensverhältnisse/ familiären Situationen, eine Chance haben, an der digitalen Gesellschaft datenschutzgerecht teilhaben zu können.

2.15 Zertifizierung – Quo vadis?

Seit dem Inkrafttreten der DS-GVO wurde noch kein Verarbeitungsprozess bei einem Verantwortlichen oder Auftragsverarbeiter zertifiziert. Woran liegt das? Der Beitrag skizziert das Implementierungsverfahren der Zertifizierung und den derzeitigen Stand der Entwicklung.

Die Datenschutz-Grundverordnung (DS-GVO) hat die datenschutzrechtliche Zertifizierung auf europäischer Ebene eingeführt. Die Zertifizierung dient dem Nachweis, dass die Vorgaben der DS-GVO im Umgang mit personenbezogenen Daten eingehalten werden. Anders als bei den sonst bekannten Zertifizierungen sollen nach der DS-GVO nicht Produkte, wie beispielsweise bestimmte Programme oder Dienstleistungen, sondern Verarbeitungsprozesse zertifiziert werden. Mit Datenschutzsiegeln und -prüfzeichen soll den betroffenen Personen ein rascher Überblick über das Datenschutzniveau gegeben werden.
Die Datenschutzaufsichtsbehörden können keine Zertifizierungsstelle nach der DS-GVO sein – also auch nicht der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit. Er akkreditiert vielmehr als zuständige Aufsichtsbehörde andere Stellen als Zertifizierungsstellen (vergleiche Art. 58 Abs. 3 Buchstabe e) DS-GVO), dazu weiter unten mehr.
Zwar berührt eine Zertifizierung nicht die Aufgaben und Befugnisse der Aufsichtsbehörde, Art. 42 Abs. 4 DS-GVO, sie erleichtert aber ihre Arbeit und auch den Nachweis, dass die datenschutzrechtlichen Grundsätze nach Art. 5 Abs. 1 DS-GVO sowie die sonstigen Anforderungen der Verordnung eingehalten werden.
Allerdings wurde seit dem Inkrafttreten der DS-GVO noch kein Verarbeitungsprozess bei einem Verantwortlichen oder Auftragsverarbeiter zertifiziert. Woran liegt das?
Das zugrundeliegende Verfahren ist kompliziert und es gab keine Erfahrungen, auf die man zurückgreifen konnte.

Die Kriterien, nach denen zertifiziert werden soll, müssen gemäß Art. 42 Abs. 5 DS-GVO entweder von der zuständigen Aufsichtsbehörde oder durch den Europäischen Datenschutzausschuss genehmigt werden. Um die Kriterien genehmigen zu lassen, muss ein sogenanntes Konformitätsbewertungsprogramm (= Zertifizierungsprogramm) erstellt werden. Dieses ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) einzureichen. Die DAkkS ist die nationale Akkreditierungsstelle gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates. In einem koordinierten Verfahren erfolgt die Prüfung durch die DAkkS und die zuständige Aufsichtsbehörde. Dieses Zertifizierungsprogramm enthält als wesentlichen Teil die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen, die gemäß Art. 57 Abs. 1 Buchstabe n) DS-GVO in Verbindung mit Art. 42 Abs. 5 DS-GVO entweder von der zuständigen Datenschutzaufsichtsbehörde genehmigt werden oder (in der Regel über die zuständige Aufsichtsbehörde) dem Europäischen Datenschutzausschuss zur Genehmigung beziehungsweise Billigung gemäß Art. 63, 64 Abs. 1 Buchstabe c) DS-GVO zu übermitteln sind.
Erste Anträge für derartige Programme sind auch in Deutschland bereits eingegangen. Antragsteller aus Thüringen waren im Berichtszeitraum nicht dabei. Bislang wurde noch kein Zertifizierungsprogramm nach Art. 42. Abs. 5 DS-GVO genehmigt. Die Aufsichtsbehörden erarbeiten in einem Arbeitskreis derzeit ein Dokument „Anforderungen an Zertifizierungsprogramme“ (vergleiche https://www.datenschutz-konferenz-online.de/media/pr/20210203_%2020201030_protokoll_100_100.pdf), mit dessen Veröffentlichung im Jahr 2021 zu rechnen ist. Es soll die Erstellung von rechtskonformen Zertifizierungsprogrammen erleichtern.
Erst wenn ein von der zuständigen Datenschutzaufsichtsbehörde genehmigtes Zertifizierungsprogramm vorliegt, ist die Akkreditierung von Zertifizierungsstellen möglich. Die DAkkS akkreditiert als Akkreditierungsstelle die Zertifizierungsstellen gemeinsam mit der zuständigen Datenschutzaufsichtsbehörde. Die zuständige Datenschutzaufsichtsbehörde erteilt der Zertifizierungsstelle in einem eigenständigen Verfahren auf Grundlage dieser gemeinsamen Akkreditierung die Befugnis, als solche tätig werden zu dürfen. Der Antrag auf Akkreditierung wird schriftlich bei der DAkkS gestellt. Dort steht ein entsprechendes Formular bereit. Die DAkkS informiert umgehend die zuständige Aufsichtsbehörde über den Antrag und übermittelt ihr die entsprechenden Unterlagen. Die zuständige Aufsichtsbehörde wird als

Befugnis erteilende Behörde in das Akkreditierungsverfahren eingebunden.
Die Zertifizierungsstelle muss die Anforderungen des Art. 43 Abs. 2 DS-GVO erfüllen. Das heißt, sie muss unter anderem ihre Unabhängigkeit und ihr Fachwissen nachweisen und sich verpflichten, das genehmigte Zertifizierungsprogramm einzuhalten. Nach Art. 42 Abs. 3 DS-GVO erfolgt die Akkreditierung aufgrund von vorher festgelegten Anforderungen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065 erlassen (vergleiche https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf). Dabei wurden auch die „EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" vom 4. Juni 2019 beachtet.
Sobald eine Zertifizierungsstelle nach Art. 43 DS-GVO akkreditiert ist, kann mit der Zertifizierung von Verarbeitungsprozessen begonnen werden. Es bleibt abzuwarten, wann das dargestellte Verfahren zum ersten Mal erfolgreich durchlaufen wird und die ersten Verarbeitungsprozesse bei Verantwortlichen oder Auftragsverarbeiter zertifiziert werden können.

2.16 Irrtümer zur DS-GVO: Der TLfDI klärt auf

Im Berichtszeitraum konnte der TLfDI zwei häufige Irrtümer aufklären. Zum einen muss eine neue Einwilligung eingeholt werden bei einem SEPA-Mandat, wenn sich die Bankverbindung ändert und zum anderen ist auch bei der Anhörung stets der Erforderlichkeitsgrundsatz zu beachten. Im letzteren Fall musste der TLfDI eine Verwarnung erlassen, da bereits eine rechtswidrige Datenverarbeitung erfolgte.

Wird die Bank gewechselt, ändert sich auch die Bankverbindung. Bei einem Lastschriftmandat, auch SEPA-Mandat genannt, kommt die Frage auf, ob eine neue Einwilligungserklärung eingeholt werden muss, wenn eine Änderungsmitteilung seitens der Bank über den Wechsel erfolgt ist. Mit dieser Frage wandte sich eine Kommune an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Kommune hatte sich zu Recht an den TLfDI gewandt, denn in der Praxis wird davon ausgegangen, dass

keine neue Einwilligung vom Kunden eingeholt werden muss aufgrund der erfolgten Änderungsmitteilung. Diese Annahme ist jedoch ein Irrtum, denn das Gegenteil ist der Fall. Es ist zwingend eine neue Einwilligungserklärung über das SEPA-Mandat einzuholen. Grund dafür ist der Art. 6 Abs. 1 Satz 1 Buchstabe a) in Verbindung mit Art. 7 Abs. 1 Datenschutz-Grundverordnung (DS-GVO).
Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO ist die Verarbeitung nur rechtmäßig, wenn die betroffene Person ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Die Bedingungen für die Einwilligung sind in Art. 7 DS-GVO geregelt. So regelt Art. 7 Abs. 1 DS-GVO Folgendes: Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
Konkret bedeutet dies für das SEPA-Mandat, dass der Kunde in die Verarbeitung seiner personenbezogenen Daten, wozu die bisherige Bankverbindung zählt, einwilligen musste. Ändert sich nun die Bankverbindung, dann handelt es sich um neue personenbezogene Daten. Dies hat zur Folge, dass die betroffene Person neu in die Verarbeitung dieser Daten einwilligen muss. Denn Art. 7 Abs. 1 DS-GVO sieht explizit vor, dass – wenn die Verarbeitung auf einer Einwilligung beruht – der Verantwortliche nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Zwar bleibt bei einer Änderung der Bankverbindung der Kontext an sich gleich, also die Kategorie Bankverbindung, jedoch verändern sich die personenbezogenen Daten. Die Kommune muss dann nachweisen können, dass der Kunde eben in die Verarbeitung seiner **neuen** Bankverbindung eingewilligt hat. Auch wenn seitens der Bank eine schriftliche Information über die neue Bankverbindung an die Kommune erfolgt ist, stellt diese keine Einwilligung im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO dar, die gemäß Art. 7 Abs. 1 DS-GVO den Nachweis in die Verarbeitung der personenbezogenen Daten belegt. Der TLfDI teilte dies der Kommune im Rahmen seiner Beratungspflicht mit und konnte einen weiteren Rechtsirrtum aufklären.
In einem anderen Fall, der beim TLfDI einging, musste der TLfDI eine Verwarnung gegenüber einer Kommune aussprechen, da diese bereits irrtümlich gehandelt hatte. Denn sie ging fälschlicherweise davon aus, dass es im Rahmen einer Anhörung zur Aufklärung der Tierhaltung

und Beweidung erforderlich war, personenbezogene Daten eines Anzeigeerstatters gegenüber dem Anzuhörenden zu offenbaren, obwohl der Kommune bekannt war, dass es in der Vergangenheit zu Bedrohungen gegenüber dem Anzeigeerstatter kam. Darüber hinaus hatte die Kommune in der Anhörung personenbezogene Informationen eines anderen Ermittlungsverfahrens offenbart und zusätzlich suggeriert, dass es sich hier auch um denselben Anzeigeerstatter handele. Die zusätzlichen Daten und Informationen hatten jedoch nichts mit der gegenständlichen Aufklärung der Tierhaltung und Beweidung zu tun, für die die Anhörung durchgeführt wurde.
Die Kommune hat in ihrer Stellungnahme an den TLfDI eingeräumt, dass ein Verstoß gegen Art. 6 Abs. 1 Satz 1 Buchstabe e) in Verbindung mit Abs. 2 und 3 Satz 1 DS-GVO und § 16 Abs. 1 sowie § 18 Thüringer Datenschutzgesetz (ThürDSG) vorlag, da eine Rechtsgrundlage zur Übermittlung des Namens sowie die Erforderlichkeit zur Namensnennung nicht gegeben war.
Nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO ist die Verarbeitung rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die Mitgliedstaaten können gemäß Art. 6 Abs. 2 DS-GVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DS-GVO in Bezug auf die Verarbeitung zur Erfüllung von Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX der DS-GVO. Die Rechtsgrundlage für die Verarbeitungen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO wird nach Art. 6 Abs. 3 Satz 1 DS-GVO festgelegt durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.
Die Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe e) in Verbindung mit Abs. 2 und 3 Satz 1 DS-GVO wurde in § 16 Abs. 1 ThürDSG umgesetzt. Gemäß § 16 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Nach § 18 Abs. 1 Satz 1 ThürDSG trägt die

Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten die übermittelnde Stelle.
Für die Verarbeitung nach § 16 Abs. 1 ThürDSG reicht es jedoch allein nicht aus, ob es sich um eine im öffentlichen Interesse liegende Aufgabe oder um eine Verarbeitung in Ausübung öffentlicher Gewalt handelt, sondern diese muss auch erforderlich sein, sodass der Grundsatz der Verhältnismäßigkeit gewahrt wird.
Der TLfDI hatte es im hier zu entscheidenden Fall jedoch als nicht erwiesen gesehen, dass die namentliche Offenlegung des Anzeigeerstatters im Rahmen der Anhörung erforderlich war. Denn es ist immer zwischen dem Persönlichkeitsrecht der betroffenen Person und der Erforderlichkeit der Offenlegung der personenbezogenen Daten abzuwägen, das hier zugunsten des Anzeigeerstatters zu gewichten war. In der Anhörung ging es nämlich nicht um den Anzeigeerstatter, sondern um die Aufklärung der Tierhaltung und Beweidung. Ein milderes, aber gleich effizientes Mittel wäre es in diesem Fall gewesen, dem Anzuhörenden mitzuteilen, dass aufgrund von Hinweisen, die bei der Kommune eingingen, in der Sache ermittelt wird. Weil die Kommune rechtswidrig den Namen des Anzeigeerstatters offenbart hatte, kam sie zudem der ihr obliegenden Verantwortung gemäß § 18 Abs. 1 Satz 1 ThürDSG für die Übermittlung nicht im gebotenen Umfang nach.
Des Weiteren hatte die Kommune neben der rechtswidrigen Offenlegung des Anzeigeerstatters dem Anzuhörenden zusätzlich den Namen eines anderen Tierhalters offenbart, zu dem mehrere Anzeigen eingingen, und darüber hinaus suggeriert, dass es sich in diesem Fall um denselben Anzeigeerstatter handelte. Nach Auffassung des TLfDI war es nicht von Belang, die anderen Anzeigen, aufgrund derer Ermittlungen liefen, zum Inhalt der Anhörung gegen den Tierhalter zu machen, zumal hierfür auch keine Rechtgrundlage vorlag.
Aufgrund der begangenen Rechtsverstöße hat der TLfDI die Kommune gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt. Zudem musste die Kommune dem TLfDI nachweisen, dass die Mitarbeiter im künftigen Umgang mit personenbezogenen Daten sensibilisiert werden.

2.17 Ordnungswidrigkeitenverfahren beim TLfDI

Von online frei einsehbaren Mieterlisten, privaten Videoüberwachungsanlagen mit 24-Stunden-Betrieb und Fotos von Polizeieinsät-

zen in WhatsApp-Gruppen – die Arbeit des TLfDI in Bußgeldverfahren ist so vielseitig wie das Leben selbst. Dabei ist das Ziel des Bußgeldverfahrens ebenso wie das des Verwaltungsverfahrens immer auch die Sachverhaltsaufklärung.

Nicht schlecht staunten die Mieter eines Mehrfamilienhauses einer Kleinstadt im Norden Thüringens, als sie ihre Namen, die Lage und die Größe der von ihnen bewohnten Wohnung, den Mietbeginn sowie die monatliche Kalt- beziehungsweise Warmmiete tabellarisch erfasst in einer sogenannten „Mieterübersicht“ in einem öffentlich abrufbaren Exposé auf der Webseite eines Immobilienmaklers wiederfanden. Auf eine entsprechende anonyme Anzeige hin wurde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) umgehend ein Bußgeldverfahren gegen den Immobilienmakler als Verantwortlichen gemäß Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) eingeleitet.
Der TLfDI ist gemäß § 61 Abs. 1 und 6 Thüringer Datenschutzgesetz (ThürDSG) zuständig für die Verfolgung von Ordnungswidrigkeiten nach Art. 83 DS-GVO in Verbindung mit § 41 Abs. 1 Bundesdatenschutzgesetz (BDSG) sowie nach dem ThürDSG selbst, soweit die Ordnungswidrigkeiten gemäß § 37 Abs. 1 Ziffer 1 Ordnungswidrigkeitengesetz (OWiG) im Freistaat Thüringen begangen wurden. Hierbei ist der TLfDI in der Regel auf die Verfolgung von Ordnungswidrigkeiten im nicht-öffentlichen Bereich beschränkt, da der Thüringer Gesetzgeber auf Grundlage der Regelungsbefugnis des Art. 83 Abs. 7 DS-GVO mit § 61 Abs. 4 ThürDSG bestimmt hat, dass gegen öffentliche Stellen keine Geldbußen verhängt werden. Von diesem Privileg sind lediglich diejenigen öffentliche Stellen ausgenommen und damit der Privatwirtschaft gleichgesetzt, die am Wettbewerb teilnehmen, vergleiche § 26 ThürDSG. Auch ist nach § 61 Abs. 1 ThürDSG als weitere Ausnahme die Verhängung von Geldbußen gegenüber Mitarbeitern öffentlicher Stellen möglich, wenn diese vorsätzlich zu dienstlichen Zwecken gegen das Datenschutzrecht verstoßen. Verstoßen Mitarbeiter öffentlicher Stellen hingegen *zu eigenen Zwecken* gegen datenschutzrechtliche Regelungen, werden diese Mitarbeiter als eigene Verantwortliche nach den Regelungen der DS-GVO verfolgt, da sie durch ihr Handeln selber Mittel und Zwecke der Datenverarbeitung festgelegt haben, Art. 4 Nr. 7 DS-GVO (sogenannter Exzess).
Doch nicht immer erreichen den TLfDI nur anonyme Anzeigen wie im Fall des Immobilienmaklers, sondern weit häufiger Ordnungswid-

rigkeitenanzeigen, die betroffene Personen bei der Polizei eingereicht haben und von dieser zuständigkeitshalber an den TLfDI abgegeben werden. Häufig kommt es auch vor, dass zunächst die Thüringer Staatsanwaltschaften Ermittlungsverfahren wegen Straftaten gegen Verantwortliche durchführen und nach deren Einstellung die Verfahren an den TLfDI zur Verfolgung einer Ordnungswidrigkeit abgeben. Oftmals werden Ordnungswidrigkeitenverfahren auch einfach im Anschluss an ein Verwaltungsverfahren, die durch den TLfDI selbst bearbeitet wurden, eingeleitet.
Ob ein solches Verfahren eingeleitet wird, hängt davon ab, ob gemäß § 152 Abs. 2 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 OWiG zureichende tatsächliche Anhaltspunkte für eine Ordnungswidrigkeit vorliegen, also ein Anfangsverdacht besteht. Aufgrund des im Ermittlungsverfahren geltenden Opportunitätsgrundsatzes gemäß § 47 Abs. 1 Satz 1 OWiG steht die Einleitung des Bußgeldverfahrens im pflichtgemäßen Ermessen des TLfDI. Er entscheidet insoweit, ob die Ahndung einer Ordnungswidrigkeit im öffentlichen Interesse geboten ist. Eine Pflicht zur Verfahrenseinleitung wegen Ermessensreduzierung auf Null oder auf Antrag besteht hingegen nicht. Da die Verfahrenseinleitung nicht auf die Ahndung, sondern auf die Sachverhaltsaufklärung gerichtet ist, der dann die Ahndung folgen kann, reichen in der Regel relativ geringe Anforderungen an den Anfangsverdacht aus. Im Fall des Immobilienmaklers war dieser ohne weiteres zu bejahen, da die Daten der Mieter bei einer Überprüfung durch den TLfDI im Anschluss an den Eingang der anonymen Anzeige noch immer öffentlich abrufbar waren und die Wahrscheinlichkeit sehr groß war, dass die Veröffentlichung der Daten unrechtmäßig erfolgte.
Nach Einleitung des Ordnungswidrigkeitenverfahrens geht der TLfDI den Anhaltspunkten für das Vorliegen einer Ordnungswidrigkeit im sogenannten Vorverfahren nach. Ziel des Verfahrens ist die Feststellung, ob eine Bußgeldentscheidung zu erlassen oder das Verfahren einzustellen ist. Hierfür wird beim TLfDI ein Ermittlungsverfahren nach den Grundsätzen des Strafverfahrens durchgeführt, welches in sinngemäßer Anwendung des § 160 StPO im Wesentlichen die Aufklärung des Sachverhalts und die Beweissicherung verfolgt. Obgleich der Gesetzgeber eine freie Gestaltung des Ermittlungsverfahrens vorsieht, wird in aller Regel auf Ermittlungshandlungen wie die Vernehmung von Zeugen, auf die Auskünfte anderer Behörden oder die Beiziehung entsprechender Akten zurückgegriffen. Eher selten ist dage-

gen die Beschlagnahme von Beweisgegenständen oder gar die Durchsuchung beim Betroffenen anzutreffen, obgleich der TLfDI die Möglichkeit hat, hiervon Gebrauch zu machen und diese Maßnahmen, wenn notwendig, auch einsetzt. Soweit erforderlich, stehen auch die Technikexperten des entsprechenden Referats beim TLfDI mit Rat und Tat zur Seite, geben Stellungnahmen ab und sichern Beweise. So auch im Falle des Immobilienmaklers, bei dem das Technikreferat bereits frühzeitig die „Mieterübersicht" auf der Webseite aus technischer Sicht analysiert und zur Verwendung als Beweis für das Bußgeldverfahren gespeichert hatte.

Das Vorverfahren endet beim TLfDI schließlich – je nach Ergebnis der durchgeführten Ermittlungen – mit der Einstellung des Bußgeldverfahrens, einer Verwarnung, wenn dies zulässig oder geboten ist oder mit dem Erlass eines Bußgeldbescheides. Gemäß § 41 Abs. 2 Satz 2 BDSG finden bei Bußgeldverfahren wegen Verstößen gegen Art. 83 Abs. 4 bis 6 DS-GVO unter anderem die Vorschriften der §§ 56 bis 58 OWiG (Verwarnung durch die Verwaltungsbehörde) keine Anwendung. Die Erteilung einer Verwarnung nach dem OWiG ist daher bei DS-GVO-Bußgeldverfahren ausgeschlossen.

Der Thüringer Gesetzgeber hat hingegen im Thüringer Datenschutzgesetz (ThürDSG) die Anwendbarkeit der §§ 56 bis 58 OWiG nicht ausgeschlossen. Voraussetzungen für eine Verwarnung ist, dass die begangene Ordnungswidrigkeit als geringfügig einzuordnen ist. Dies richtet sich nach der Bedeutung der Handlung und dem Grad der Vorwerfbarkeit, wobei die Gesamtbetrachtung entscheidet (vgl. Gürtler in Göhler / Ordnungswidrigkeitengesetz, 17. Aufl. 2017, § 56 Rn. 6). Da aber wegen der Regelung in § 10 OWiG nur vorsätzliches Handeln nach dem ThürDSG als Ordnungswidrigkeit geahndet werden kann, ist die Verwarnung in aller Regel nicht das Mittel der Wahl.

Ergeben die Ermittlungen keinen zum Erlass eines Bußgeldbescheides hinreichenden Tatverdacht gegen den Betroffenen, kann also die Unschuldsvermutung nicht widerlegt werden, so ist das Bußgeldverfahren aus tatsächlichen Gründen gemäß § 170 Abs. 2 Satz 1 StPO in Verbindung mit § 46 Abs. 1 OWiG einzustellen.

Möglich, in der Praxis aber weitaus weniger relevant, ist darüber hinaus auch eine Einstellung des Verfahrens aus rechtlichen Gründen wegen des Bestehens eines dauernden Verfolgungshindernisses. Wichtigstes Beispiel ist in diesem Zusammenhang der Eintritt der Verfolgungsverjährung. Schließlich kann der TLfDI das Verfahren im Rahmen einer pflichtgemäßen Ermessensentscheidung nach § 47 Abs. 1

Satz 1 OWiG auch dann einstellen, soweit er eine Ahndung trotz feststehenden Tatnachweises für nicht geboten erachtet.
Im Fall des Immobilienmaklers kam keine der vorgenannten Einstellungsgründe in Betracht, da die „Mieterübersicht“ über den gesamten Verlauf des Ermittlungsverfahrens online abrufbar war, es sich also nicht lediglich um kurzfristiges Versehen handelte und darüber hinaus auch der Tatnachweis als gesichert galt.
Kommt im Bußgeldverfahren weder eine Einstellung noch eine Verwarnung in Betracht, ergeht gegen den Betroffenen nach vollständiger Aufklärung des Sachverhalts ein Bußgeldbescheid mit entsprechender Festsetzung der Geldbuße. Dem Betroffenen ist allerdings vor Erlass einer Bußgeldentscheidung gemäß § 55 Abs. 1 OWiG, § 163a Abs. 1 StPO Gelegenheit zu geben, sich zur Beschuldigung zu äußern. Die Anhörung soll dem Betroffenen die Möglichkeit des rechtlichen Gehörs zum Tatvorwurf der Ordnungswidrigkeit und bezüglich der Rechtsfolgen zu seiner wirtschaftlichen Leistungsfähigkeit geben. Der Immobilienmakler im Fall der „Mieterübersicht“ hatte hiervon Gebrauch gemacht und die Ordnungswidrigkeit im Rahmen der Anhörung gegenüber dem TLfDI eingeräumt und sich für die unrechtmäßige Veröffentlichung der personenbezogenen Daten der Mieter entschuldigt. Dies wurde bei der Zumessung der Geldbuße durch den TLfDI, welcher gemäß Art. 83 Abs. 5 DS-GVO Geldbußen bis zu einer Höhe von 20.000.000 Euro bzw. im Falle von Unternehmen bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängen kann, ebenso gebührend berücksichtigt wie die Art, Schwere und Dauer des Verstoßes, der Kooperation mit der Aufsichtsbehörde, die hohe Anzahl der von der Verarbeitung betroffenen Personen sowie die fahrlässige Begehungsweise der Tat. Das hier verhängte Bußgeld im vierstelligen Bereich war damit im Ergebnis wirksam, verhältnismäßig und abschreckend im Sinne von Art. 83 Abs. 1 DS-GVO.
Doch warum war die Veröffentlichung der Mieterdaten durch den Immobilienmakler überhaupt rechtswidrig? Nach der Systematik der DS-GVO ist eine Datenverarbeitung grundsätzlich untersagt, außer sie wird durch einen oder mehrere Erlaubnistatbestände des Art. 6 DS-GVO ausdrücklich gestattet. Hierbei spricht man von einem sogenannten Verbot mit Erlaubnisvorbehalt. Hinzu kommt das Prinzip der sogenannten Zweckbindung nach Art. 5 Buchstabe b) DS-GVO, wonach personenbezogene Daten nicht für andere als die im Vorhinein festgelegten Zwecke verwendet werden dürfen. Vorliegend kamen

eine Reihe von Erlaubnistatbeständen in Betracht, deren Vorliegen letztlich jedoch zu verneinen war. Zu prüfen war beispielsweise, ob die Verarbeitung der personenbezogenen Daten zur Erfüllung eines Vertrages beziehungsweise zur Durchführung vorvertraglicher Maßnahmen nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO erforderlich war. Unstreitig war hier ein Vertragsverhältnis in Gestalt eines Maklervertrages zu bejahen, allerdings nur im Verhältnis zwischen dem Immobilienmakler und dem Eigentümer der Mietwohnungen. Dieser wiederum hatte entsprechende Mietverträge mit den Mietern geschlossen. Der Immobilienmakler war als Dritter von dieser Konstellation jedoch nicht umfasst. Darüber hinaus wäre es weder zur Erfüllung eines Miet- noch des Maklervertrages erforderlich gewesen, die personenbezogenen Daten im Rahmen eines Online-Exposés zu verarbeiten. Weiter war zu prüfen, ob die Verarbeitung möglicherweise zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO erforderlich war, soweit nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwogen. Zwar war es hier wirtschaftlich betrachtet durchaus nachvollziehbar, dass potentielle Kaufinteressenten der Immobilie einen Ausblick auf die zu erwartenden Mieteinnahmen erhalten, hierzu bedurfte es jedoch nicht der Angabe der Namen der entsprechenden Mieter. Letztlich war es daher nicht erforderlich, die Mieterdaten zu veröffentlichen. In jedem Fall standen die schutzwürdigen Interessen der Mieter der Veröffentlichung entgegen. Als einzig ernsthaft in Betracht zu ziehende Möglichkeit, um von einer Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten durch den Immobilienmakler auszugehen, kam hier nur eine Einwilligung der Mieter nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Betracht. Hierfür wäre es jedoch erforderlich gewesen, dass diese vor Veröffentlichung ihrer Daten in die entsprechende Datenverarbeitung unter Nennung des Zweckes der Verarbeitung eingewilligt hätten. Eine solche Einwilligung lag dem Immobilienmakler jedoch zu keinem Zeitpunkt vor. Im Ergebnis stellte die Veröffentlichung der Mieterdaten auf der Internetseite des Maklers daher eine unrechtmäßige Verarbeitung von personenbezogenen Daten dar.

Doch nicht nur unrechtmäßige Veröffentlichungen von personenbezogenen Daten im Internet beschäftigen den TLfDI wie im zuvor gezeigten Beispiel. Weitaus häufiger sind Videoüberwachungsanlagen im privaten Bereich Gegenstand von Bußgeldverfahren. So auch im Fall des Eigentümers eines Wohnhauses in einer Stadt im Süden Thürin-

gens. Dieser betrieb eine nicht schwenkbare und nicht zoomfähige Überwachungskamera mit Nachtsichtfunktion, welche permanent Live-Bilder auf das Smartphone des verantwortlichen Hauseigentümers übertrug beziehungsweise übertragen konnte, ohne jedoch die Aufzeichnung dauerhaft zu speichern. Dabei war die Kamera am Dachkasten des Gebäudes angebracht und auf den Außenbereich vor dem Wohnhaus derart ausgerichtet, dass neben dem Eingangstor und der Klingel auch ein circa zwei Quadratmeter großer öffentlicher Bereich vor dem Tor erfasst wurde. Vom Sichtbereich der Kamera waren ein Teil der Straße, der Parkfläche sowie des Gehweges mittels Software ausgeblendet. Ein Hinweisschild zur Kamera und zu den Betroffenenrechten hatte der Verantwortliche nicht angebracht. Der TLfDI verhängte hier schließlich ein Bußgeld in Höhe von mehreren hundert Euro, da nach dem Ergebnis der Ermittlungen festzustellen war, dass trotz der softwareseitigen teilweisen Ausblendung noch immer eine Kameraüberwachung des öffentlichen Bereichs stattfand. Die so stattfindende Verarbeitung personenbezogener Daten konnte der Verantwortliche nicht auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO stützen, da diese allein schon aufgrund der hohen Anzahl betroffener Personen nicht eingeholt werden konnte. Überdies müsste diese vor (!) Betreten des videoüberwachten Bereiches eingeholt werden und auch im Übrigen den hohen Voraussetzungen der datenschutzrechtlichen Einwilligung genügen.
Aufgrund der Einlassungen des Verantwortlichen im Rahmen der Anhörung war hier jedoch insbesondere zu prüfen, ob möglicherweise eine Datenverarbeitung zur Wahrung berechtigter Interessen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO vorlag. Der Verantwortliche hatte nämlich vorgetragen, dass mittels der Kamera die Eingangstür insbesondere beim Klingeln überwacht werden sollte und die Nachtsichtfunktion, die von außen durch die Infrarotsensoren deutlich zu erkennen waren, vor Einbruchsversuchen durch Abschreckung schützen sollte. Der TLfDI verneinte hier schließlich die Erforderlichkeit der Überwachung, da diese Tag und Nacht stattfand, also auch dann, wenn weder der Verantwortliche noch andere Familienmitglieder zu Hause waren. Auch das Argument der Abschreckung vor Einbrüchen vermochte nicht zu überzeugen, da der Verantwortliche eine konkrete Gefahrenlage (etwa aufgrund früherer Einbrüche) nicht nachgewiesen hatte. Die Videoüberwachung war im Ergebnis daher zur Zweckerfüllung weder erforderlich noch geeignet, womit eine unrechtmäßige Verarbeitung von personenbezogenen Daten vorlag. Die-

ses Beispiel zeigt, dass die Videoüberwachung nur in sehr engen Grenzen zulässig ist. Nämlich dann, wenn die Kamera nur durch Betätigung der Klingel aktiviert wird, eine Bildübertragung allein in die Wohnung erfolgt, bei der geklingelt wurde, die Bildübertragung nach spätestens einer Minute unterbrochen wird und die Anlage nicht das dauerhafte Aufzeichnen von Bildern ermöglicht.
Neben den Betreibern von Videoüberwachungsanlagen muss sich der TLfDI in Bußgeldverfahren aber auch regelmäßig mit Ordnungshütern beschäftigen. Fälle, in denen Polizeibeamte aus rein privaten Gründen Personen in polizeilichen Recherche- und IT-Systemen abfragen, waren schon häufiger Gegenstand von Bußgeldverfahren und wurden zum Teil mit Bußgeldern bis in den vierstelligen Bereich hinein geahndet. Vollkommen neu war dem TLfDI bis dato jedoch ein Sachverhalt, in dem ein Polizeibeamter während des Dienstes innerhalb einer WhatsApp-Gruppe mehrfach Fotos von Polizeieinsätzen mit teilweise hämischen Kommentaren versendet hatte. Auf einem Foto war eine mit Fäkalien hinterlassene Toilette zu sehen, auf einem anderen ein Verkehrsunfall. Während beim ersten Foto durch den Kommentar des Polizeibeamten ein Bezug zu einer Familie hergestellt werden konnte, bei der es zu dem Polizeieinsatz gekommen war, waren auf dem zweiten Foto Firmenaufschriften der betroffenen Fahrzeuge, Kennzeichen sowie Personen erkennbar. Der TLfDI stellte im Ergebnis fest, dass der betroffene Polizeibeamte in beiden Fällen unbefugt personenbezogene Daten erhoben und verarbeitet hatte, indem er die Fotos auf seinem Smartphone gespeichert und mittels des Messenger-Dienstes WhatsApp an Dritte übermittelt hatte. Hierbei lag ein sogenannter „Exzess“ vor, bei dem der Polizeibeamte dienstlich erlangte Informationen zu rein privaten Zwecken (weiter-)verarbeitet hatte. Da diese Handlungen nicht mehr der dienstlichen Tätigkeit zuzurechnen waren, handelte der Polizeibeamte als eigener Verantwortlicher, weshalb dieser Fall trotz des Bezugs zur Thüringer Polizei dem nicht-öffentlichen Bereich zuzuordnen ist (siehe oben.)
So unterschiedlich die Sachverhalte der zuvor dargestellten Fälle waren, so unterschiedlich gestalteten sich auch die Verfahren. Während der Immobilienmakler und der Polizeibeamte die verhängten Bußgelder sofort akzeptierten und auch bezahlten, erhob der Betreiber der Videoüberwachungsanlage Einspruch gegen den Bußgeldbescheid.
Der **Einspruch nach § 67 OWiG** ist der statthafte Rechtsbehelf des Bußgeldverfahrens gegen den Bußgeldbescheid. Dieser verhindert den Eintritt der Rechtskraft des Bußgeldbescheides und insoweit auch

dessen Vollstreckbarkeit. Der Betroffene hat hier nochmals die Möglichkeit Stellung zu nehmen. Der Einspruch eröffnet das Zwischenverfahren gemäß § 69 Abs. 2 und 3 OWiG, bei dem der TLfDI prüft, ob er den Bußgeldbescheid aufrechterhält oder zurücknimmt. Zu diesem Zweck kann er weitere Ermittlungen durchführen oder dem Betroffenen Gelegenheit geben, sich dazu zu äußern, ob und welche Tatsachen und Beweismittel er im weiteren Verfahren vorbringen will. Nimmt der TLfDI den Bußgeldbescheid nicht zurück, übersendet er die Bußgeldakte über die Staatsanwaltschaft an das in Thüringen hierfür einzig zuständige Amtsgericht Erfurt. Mit Übergabe der Akte gehen sämtliche Aufgaben auf die Staatsanwaltschaft über. Diese entscheidet sodann selbst, ob sie das Verfahren einstellt, weitere Ermittlungen durchführt oder die Bußgeldakte dem Richter beim Amtsgericht vorlegt, wobei eine Einstellung des Verfahrens durch die Staatsanwaltschaft nur mit Zustimmung des TLfDI möglich ist, § 41, Abs. 2 Satz 3 BSDG. Durch den Übergang der Aufgaben auf die Staatsanwaltschaft ist der TLfDI nicht unmittelbar an dem sich an das Zwischenverfahren anschließenden Verfahren vor dem Amtsgericht beteiligt. Der Richter am Amtsgericht entscheidet schließlich auf Grundlage des im Bußgeldbescheid geschilderten Tathergangs, ob eine Ordnungswidrigkeit vorliegt, keine Verfahrenshindernisse vorliegen und eine Ahndung geboten erscheint. Im Fall des Betreibers der Videoüberwachungsanlage hat der TLfDI auf den Einspruch hin den Bußgeldbescheid nach erneuter Überprüfung nicht zurückgenommen und die Bußgeldakte über die Staatsanwaltschaft Erfurt an das Amtsgericht Erfurt versendet. Nachdem dieses bereits einen Termin zur Hauptverhandlung bestimmt hatte, nahm der Betroffene seinen Einspruch jedoch zurück und bezahlte umgehend das Bußgeld.
Damit endete das Bußgeldverfahren – wie viele andere auch – im Berichtszeitraum 2020 mit einem rechtskräftigen Bußgeldbescheid. Dabei stellt der Erlass eines Bußgeldbescheids keineswegs die Regel dar. Viele Verfahren werden nach dem Ergebnis der durchgeführten Ermittlungen eingestellt, wenn sich ein hinreichender Tatverdacht nicht ergeben hat.

2.18 Reichsbürger beim TLfDI: Wenn Argumente nicht mehr helfen

Nach § 8 Abs. 1 ThürDSG kann sich jede Person an den TLfDI wenden, wenn sie der Ansicht ist, dass sie bei der Verarbeitung ihrer per-

sonenbezogenen Daten in ihren Rechten verletzt worden ist. Auch wenn diese Regelung für so genannte „Reichsbürger“ aus Thüringen gilt, so hat der TLfDI in den letzten Jahren Erfahrungen gesammelt, wie er mit den Anliegen dieser Menschen, die den demokratischen Rechtsstaat ablehnen und ihn sogar bekämpfen, umgeht.

In den letzten Jahren hat sich auch die Zahl der Beschwerden, die beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von so genannten Reichsbürgern oder Personen, die dieser Gruppe zugerechnet werden können, eingegangen sind, erhöht.
Die Leserin/ der Leser dieses Tätigkeitsberichts wird sich nun fragen, woran man einen Reichsbürger erkennt beziehungsweise, ob es eine allgemein gültige Definition des Begriffs „Reichsbürger“ gibt? Laut Glossar der Bundeszentrale für politische Bildung (bpb) bezeichnen sich als „Reichsbürger“ oder auch „Reichsregierungen“ mehrere sektenartige Gruppen von Rechtsextremen und Verschwörungstheoretikern. Diese Gruppen behaupten, das Grundgesetz sei eine „Fortsetzung des Krieges gegen das Deutsche Reich“ und die Bundesregierung ein von „den westlichen Siegermächten aufgezwungenes Statut der Fremdherrschaft über das Deutsche Volk“. Als Konsequenz weigern sich die Reichsbürger, Steuern zu zahlen und erkennen die deutsche Gesetzgebung nicht an. Manche stellen eigene Reisepässe und Führerscheine ihres Fantasiestaates her und ernennen sich selbst zu „Ministern“ verschiedener Regierungen.
Mit solchen „Regierungen“ oder „Ministern“ hatte der TLfDI in den letzten Jahren keinen Kontakt, es trugen aber verschiedene Personen aus dem Umfeld der Reichsbürger ihre Beschwerden beim TLfDI vor. Die meisten von ihnen ließen sich bereits deshalb zur Reichsbürgerszene zuordnen, weil sie zu ihrem Nachnamen noch einen – meist recht eigenwilligen – Namenszusatz verwendeten. Hier einige Beispiele kurioser Beschwerden und Eingaben an den TLfDI:
Ein Reichsbürger war offensichtlich mit dem Gesetz in Konflikt geraten und erkannte die Schriftstücke und Ladungen eines Thüringer Amtsgerichts nicht an. Daher leitete er seine sämtliche Gerichtspost an die Poststelle des TLfDI weiter. Dessen Aufforderungen, dies zu unterlassen, fruchteten zunächst nicht. Erst als der TLfDI gegenüber dem Reichsbürger ankündigte, dessen Gerichtspost an das Gericht postwendend zurückzusenden und diese Ankündigung auch vollzog,

ließ der Reichsbürger von seinem Versuch ab, den TLfDI als seine persönliche Poststelle einzusetzen.
Mit der Postzustellung hatte auch ein anderer „Reichsbürger-Fall“ beim TLfDI zu tun: Ein Vertreter der Reichsbürger-Szene – wiederum deutlich am entsprechenden Namenszusatz zu erkennen – beschwerte sich beim TLfDI darüber, dass die mit ihm korrespondierenden Behörden nicht den nach seiner Ansicht für ihn zutreffenden Namen auf den Schreiben verwendeten. Daher hatte er „seine Poststelle“ angewiesen, diese Behördenschreiben nicht anzunehmen. Mit diesem „Problem“ hatte auch der TLfDI dann zu „kämpfen“: Seine Eingangsbestätigung, die korrekt an den Vor- und Nachnamen des Beschwerdeführers adressiert war, kam prompt zurück – weil der Reichsbürger auch beim Schreiben des TLfDI keine Ausnahme von seiner Regel zuließ, dass ihn nur Briefe mit dem aus seiner Sicht „richtigen“ Namen erreichen durften. Der TLfDI hat dem Mann dann noch einmal mitgeteilt, dass er ihm leider nicht helfen könne, wenn er die Briefe des TLfDI nicht annimmt. Ob diese Nachricht des TLfDI den Reichsbürger jemals erreicht hat, ist nicht bekannt!
Last but not least soll hier noch von einem dritten Fall mit Reichsbürger-Bezug berichtet werden, bei dem es ebenfalls um den Empfang von Gerichtspost ging. Ein Bürger beschwerte sich über seinen Bevollmächtigten – ein hinlänglich bekannter Reichsbürger – darüber, dass ein Thüringer Amtsgericht ihn mehrfach unter einer falschen Adresse kontaktiert habe. Daraus leitete der Beschwerdeführer dann ab, eine dritte Person habe Zugang zu seinen personenbezogenen Daten erhalten, weil diese dritte Person die Schreiben des Amtsgerichts unter der Adresse erhalten hätte. Der TLfDI konnte durch Kontaktaufnahme mit dem Amtsgericht jedoch schnell und präzise nachweisen, dass dieses den Beschwerdeführer zwei Mal unter seiner falschen Adresse angeschrieben hatte. Diese beiden Schreiben waren aber jedes Mal von der Post an das Amtsgericht zurückgeleitet worden, sodass kein Dritter die personenbezogenen Daten des Beschwerdeführers aus den Gerichtsschreiben zur Kenntnis nehmen konnte. Dieses Ergebnis teilte der TLfDI dem Beschwerdeführer mit und zeigte ihm den möglichen Rechtsweg gegen den TLfDI-Bescheid auf. Dagegen hat der Beschwerdeführer nicht geklagt – auch wenn sein Bevollmächtigter nicht mit dem Inhalt des TLfDI-Bescheids einverstanden war und dies lauthals gegenüber dem TLfDI am Telefon kundtat.
Fazit: Auch wenn die geschilderten drei Fälle recht kurios anmuten und vielleicht beim Leser/ bei der Leserin dieses Tätigkeitsberichts zu

dem Gedanken führen, ob die Mitarbeitenden beim TLfDI denn nichts Besseres zu tun haben, als sich mit wirren Beschwerden von Reichsbürgern zu beschäftigen, so sollen sie drei Dinge deutlich machen:
Erstens: Gemäß § 8 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) kann sich jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs mit einer Beschwerde unmittelbar an den TLfDI wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen des Landes in ihren Rechten verletzt worden zu sein.
Zweitens: Auch dem TLfDI ist bewusst, dass er zuweilen die von ihm kontaktierten öffentlichen Stellen mit zusätzlicher Arbeit belegt – wenn sich ein Reichsbürger einmal wieder mit rechtlich oder tatsächlich fragwürdigen Beschwerden an den TLfDI gewandt hat. Zu bedenken ist dabei aber zum einen, dass auch die Vertreter aus der Reichsbürgerszene zunächst einmal uneingeschränkt das Recht haben, sich gemäß § 8 Abs. 1 ThürDSG an den TLfDI zu wenden. Zum anderen ist jedoch zu berücksichtigen, dass auch der TLfDI „seine (Thüringer) Pappenheimer“ mittlerweile kennt und sich mit legalen Mitteln zu helfen weiß, wie man sich nicht „vor den Karren“ von Reichsbürgern „spannen“ lässt.
Drittens: Auch der TLfDI hat sich in den vergangenen Jahren immer wieder die Frage gestellt, warum Reichsbürger ihn einschalten, wenn die Institution des Datenschutzbeauftragten zu einem System gehört, das sie, die Reichsbürger, eigentlich ablehnen!

2.19 Datenpannen auch in Thüringen

Sämtliche öffentliche und nicht-öffentliche Stellen müssen gegenüber der zuständigen Aufsichtsbehörde Datenschutzverletzungen melden, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat im Berichtszeitraum über 200 entsprechende Meldungen erhalten.

In der Datenschutz-Grundverordnung (DS-GVO) werden Fälle von Datenschutzverstößen unter dem Begriff der „Verletzung des Schutzes personenbezogener Daten“ zusammengefasst. Eine solche Verletzung – umgangssprachlich gelegentlich auch Datenpanne genannt – liegt vor, wenn es zu einem Vorfall kommt, der zur Vernichtung, zum

Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten kommt, welche übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
Liegt eine Verletzung des Schutzes personenbezogener Daten vor, muss die verantwortliche Stelle gemäß Art. 33 der DS-GVO unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung eine Meldung an die Aufsichtsbehörde abgeben. Sollte diese Frist von 72 Stunden nicht eingehalten werden, muss die Verzögerung zusammen mit der Meldung begründet werden.
Es ist zu beachten, dass eine Meldepflicht nur dann nicht besteht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Ein angemessenes und rechtzeitiges Reagieren im Falle einer Verletzung des Schutzes personenbezogener Daten ist wichtig, da diese zu einem physischen, materiellen oder immateriellen Schaden für natürliche Personen führen kann. Dementsprechend kann es als Ordnungswidrigkeit nach Art. 83 Abs. 4 Buchstabe a) DS-GVO geahndet werden, wenn

- eine Datenpanne nach Art. 33 Abs. 1 DS-GVO dem TLfDI als Aufsichtsbehörde nicht gemeldet wird oder
- die betroffenen Personen nach Art. 34 Abs. 1 DS-GVO bei einem voraussichtlich **hohen** Risiko für die persönlichen Rechte und Freiheiten nicht benachrichtigt werden.

Es ist insbesondere darauf hinzuweisen, dass der Verantwortliche aufgrund dieser Meldung der Verletzung des Schutzes personenbezogener Daten kein Ordnungswidrigkeitenverfahren befürchten muss, § 43 Abs. 4 Bundesdatenschutzgesetz. Insgesamt erreichten den TLfDI im Berichtszeitraum 204 Datenpannenmeldungen von öffentlichen und nicht-öffentlichen Stellen. Im nicht-öffentlichen Bereich sind die Meldungen am häufigsten von Angriffen mittels Verschlüsselungstrojanern veranlasst, welche durch das Öffnen von E-Mail-Anhängen Schadsoftware freisetzen. Ein weiterer Großteil der Meldungen ist durch offene E-Mail-Verteiler veranlasst. Dies führt regelmäßig zur unberechtigten Offenbarung von personenbezogenen Daten. Einige interessante Fälle werden in diesem Bericht näher beleuchtet.

2.20 Brexit – Über Nacht zum „datenschutzrechtlichen Drittstaat“

Mit dem Austritt des Vereinigten Königreichs aus der Europäischen Union ist das Land auch in datenschutzrechtlicher Hinsicht anders zu bewerten, nämlich als so genanntes Drittland. Verantwortliche, die personenbezogene Daten in das Vereinigte Königreich übermitteln und weiter übermitteln möchten, müssen ihre Datenverarbeitungen überprüfen und entsprechend anpassen.

Das Austrittsabkommen (Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01)) vom 12. November 2019 sah eine Übergangsphase bis zum 31. Dezember 2020 vor (Art. 126). In dieser Phase blieb das EU-Recht weiter anwendbar (Art. 127). Folglich galt auch die Datenschutz-Grundverordnung (DS-GVO) bis Ende des Jahres 2020 weiter. Während dieser Zeit durften Datenverarbeitungen auch wie bisher auf der Grundlage der DS-GVO vorgenommen werden.
Ab 1. Januar 2021 wurde das Vereinigte Königreich zu einem Drittland im Sinne von Kapitel V der DS-GVO. Für eine vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich galt eine viermonatige Übergangsfrist (die um zwei Monate verlängert werden durfte). Damit sollten Übermittlungen personenbezogener Daten in das Vereinigte Königreich Großbritannien und Nordirland für diese Übergangsperiode nicht als Übermittlungen in ein Drittland (Art. 44 DS-GVO) angesehen werden (siehe hierzu auch Beitrag 7.1 Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 28. Dezember 2020 – „Vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich – Entwurf des Brexit-Abkommens bietet viermonatige Übergangsfrist ab dem 1. Januar 2021“).
Stellt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unrechtmäßige Datenübermittlungen nach dieser Übergangsphase fest, stehen ihm auch hier die Befugnisse gemäß Art. 58 Abs. 2 DS-GVO zur Verfügung. So kann er gemäß Art. 58 Abs. 2 Buchstabe j) DS-GVO die Datenübermittlung aussetzen oder gemäß Art. 83 Abs. 5 Buchstabe c) DS-GVO im Einzelfall

eine Geldbuße verhängen, wenn Verstöße festgestellt werden. Grundsätzlich kann man davon ausgehen, dass das Vereinigte Königreich bereits ein recht hohes Datenschutzniveau aufweist. Dennoch müssen alle Datenverarbeitungen, die im Vereinigten Königreich erfolgen, auf ihre Zulässigkeit durch den Verantwortlichen überprüft werden. Dazu zählt auch, dass die Informationen, die der Verantwortliche zur Verfügung zu stellen hat, angepasst werden und nunmehr über die Datenübermittlung in ein Drittland informiert wird (Art. 13 Abs. 1 Buchstabe f) DS-GVO, Art. 14 Abs. 1 Buchstabe f) DS-GVO), dass bei einem Auskunftsbegehren einer Person ihr auch Informationen zu Datenübermittlungen in das Drittland gegeben werden (Art. 15 Abs. 1 Buchstabe c) und Abs. 2 DS-GVO). Weiterhin ist auch das Verzeichnis für Verarbeitungstätigkeiten entsprechend anzupassen (Art. 30 Abs. 1 Buchstabe d) und Buchstabe e) DS-GVO; Art. 30 Abs. 2 Buchstabe c) DS-GVO) und, solange die EU-Kommission keinen Angemessenheitsbeschluss erlassen hat, sind die Art. 44 ff. DS-GVO (Kapitel V) zu beachten. Das heißt, es sind geeignete Garantien zu schaffen, wenn nicht im Einzelfall gegebenenfalls ein Ausnahmetatbestand greift.
Auch hier sind die Auswirkungen der aktuellen Rechtsprechung des Europäischen Gerichtshofs zu berücksichtigen (siehe Beitrag 2.1), dessen grundsätzliche Ausführungen auf jeglichen Drittstaatentransfer angewendet werden können.

3. Fälle öffentlicher Bereich

© alphaspirit – stressed spam – fotolia.com

3.1 Weitergabe von Zeugendaten bei einem Verkehrsunfall

Der Personalienaustausch von Unfallbeteiligten ist gemäß § 34 Straßenverkehrsordnung erforderlich, um die Schäden eines Verkehrsunfalls zu regulieren. Zu beachten ist jedoch, dass Zeugen dem Personenkreis der Unfallbeteiligten zunächst nicht zugerechnet werden können. Daher kann die Weitergabe von Zeugendaten an Unfallbeteiligte nur mit deren Einwilligung erfolgen.

Anfang Juni 2020 hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) aufgrund einer Datenpannenmeldung davon Kenntnis erlangt, dass die Thüringer Polizeiinspektionen in Fällen von Verkehrsunfällen die Personalien von Zeugen mithilfe einer Personalienaustauschkarte erfassten und diese den Unfallbeteiligten zur Verfügung stellten. Neben der Anschrift des jeweiligen Zeugen wurden auf dieser Karte auch dessen Telefonnummer bei der Aufnahme erfasst. Aufgrund der Nutzung der Personalienaustauschkarte kam es zu einer ungewollten telefonischen Kontaktaufnahme mit einem Zeugen durch einen Geschädigten. Der Zeuge

beschwerte sich danach bei der verantwortlichen Polizeiinspektion über die Weitergabe seiner Daten an die Unfallbeteiligten.
Um die Rechtsgrundlage der Datenweitergabe von Zeugendaten bei einem Verkehrsunfall zu überprüfen, wandte sich der TLfDI an das Thüringer Ministerium für Inneres und Kommunales (TMIK). Dieses gab an, dass die Personalienaustauschkarten den Unfallbeteiligten als Serviceleistung durch die Polizei zur Verfügung gestellt werden. Grundsätzlich erachtet es der TLfDI als zulässig, wenn die Polizei als Serviceleistung den Personalienaustausch nach einem Verkehrsunfall dadurch unterstützt, dass sie entsprechende Vordrucke vorhält. Dabei tauschen die Unfallbeteiligten die Daten untereinander aus. Die Zurverfügungstellung der Vordrucke unterstützt dabei letztlich nur die rechtliche Verpflichtung der Unfallbeteiligten, selbst nach § 34 Straßenverkehrsordnung anderen am Unfallort anwesenden Beteiligten und Geschädigten den eigenen Namen und die eigene Anschrift anzugeben. Zu beachten ist jedoch, dass sich dieser Personenkreis auf die Unfallbeteiligten beschränkt. Folgt man der Definition aus § 142 Strafgesetzbuch, so ist Unfallbeteiligter jeder, dessen Verhalten nach den Umständen zur Verursachung des Unfalls beigetragen haben kann. Ein Zeuge kann diesem Personenkreis nicht zugerechnet werden.
Das TMIK nahm den Vorfall zum Anlass, die bisher in Verwendung befindliche Personalienaustauschkarte zu überarbeiten und diese den datenschutzrechtlichen Vorgaben anzupassen. Die Änderung beinhaltet nunmehr den Hinweis, dass die notwendigen Angaben unter den Unfallbeteiligten auszutauschen sind und der Datenaustausch durch die Unfallbeteiligten selbst erfolgt. Der Austausch weiterer Daten, insbesondere auch von Zeugendaten, unterliegt der Freiwilligkeit. Die an die Unfallbeteiligten zur Verfügung gestellte Personalienaustauschkarte ist nach wie vor nicht Bestandteil der polizeilichen Unfallaufnahme.

3.2 Polizeiliche Datenbanken – Zugriff nur aus dienstlichem Anlass

Polizeiliche Datenbanken enthalten eine Vielzahl personenbezogener Daten. Diese sind wichtig, um die polizeiliche Arbeit bewerkstelligen zu können. Die Zugriffe auf Datenbanken dürfen jedoch nur zur polizeilichen Aufgabenerfüllung vorgenommen werden und müssen kontrollierbar sein.

Im Berichtszeitraum gab es deutschlandweit immer wieder Medienberichte zu unerlaubten Datenbankabfragen durch einzelne Polizeibeamte, die nicht in einem dienstlichen Zusammenhang standen. Dies warf die Frage auf, ob die polizeilichen Datenbanken im ausreichenden Maße gegen missbräuchliche Zugriffe geschützt sind und wie Zugriffe kontrolliert werden.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) begann im Berichtszeitraum, die Verfahrensweise zu prüfen, wie bei der Thüringer Polizei Datenabfragen aus den polizeilichen Informationssystemen vorgenommen werden. Der TLfDI ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz Aufsichtsbehörde im Sinne des Artikels 41 der Richtlinie (EU) 2016/680.
Um zunächst die allgemeine Verfahrensweise der Thüringer Polizei hinsichtlich der Abfragen aus polizeilichen Datenbanken einer datenschutzrechtlichen Überprüfung zu unterziehen, übersandte der TLfDI der Landespolizeidirektion als zentraler Führungs- und Einsatzdienststelle einen Fragenkatalog, den diese zur Beantwortung an das Thüringer Landeskriminalamt (TLKA) weiterleitete. Das TLKA ist die Zentralstelle für das polizeiliche Informations- und Kommunikationswesen.
Der TLfDI möchte anhand des Fragebogens unter anderem in Erfahrung bringen, von welchen Endgeräten auf polizeiliche Datenbanken Zugriffe ausgeübt werden können, wie die Authentifizierung bei einer Anmeldung erfolgt, wie die Suche in den polizeilichen Datenbanken erfolgt (zum Beispiel feste Suchparameter, Abfragegrund, Dokumentationspflichten et cetera) und wie mit missbräuchlichen Datenbankabfragen umgegangen wird.
Dieser Vorgang konnte im Berichtszeitraum aufgrund der komplexen Thematik noch nicht beendet werden; die Antworten zu den vom TLfDI gestellten Fragen stehen noch aus. Über den Ausgang wird der TLfDI daher im nächsten Tätigkeitsbericht berichten.

3.3 Predictive Policing – Kleine Anfrage

Kleine Anfragen von Abgeordneten muss der TLfDI seit Inkrafttreten des ThürDSG am 15. Juni 2018 nicht mehr beantworten. Bei einer Kleinen Anfrage zum Thema „Predictive Policing“ gegenüber dem TMIK half der TLfDI aber gern freiwillig bei der Beantwortung.

Kleine Anfragen, als Ausprägung des parlamentarischen Fragerechts, sind Kontrollinstrumente gegenüber der Landesregierung. Anhand Kleiner Anfragen informieren sich beispielsweise Abgeordnete über einzelne Sachverhalte aus den Ministerien oder der ihnen unterstellten Verwaltungen, für die das Ministerium gegenüber dem Thüringer Landtag verantwortlich ist. Kleine Anfragen gemäß Art. 90 der Geschäftsordnung des Thüringer Landtags werden schriftlich gestellt und sind bei der Landtagspräsidentin einzureichen. Die Präsidentin teilt die Anfragen unverzüglich der Landesregierung mit. Das Thüringer Ministerium für Inneres und Kommunales (TMIK) erhielt im Berichtszeitraum eine Kleine Anfrage zum Thema „Predictive Policing durch die Thüringer Polizei“ (Nr. 975). Die Frist zur Beantwortung Kleiner Anfragen beträgt gemäß Art. 90 Abs. 4 Satz 1 der Geschäftsordnung des Thüringer Landtags sechs Wochen nach Eingang bei der Landesregierung.
Im Rahmen dieser Kleinen Anfrage zum Thema „Predictive Policing“ wollte der Abgeordnete unter anderem auch wissen, ob sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Einsatz einer solchen Software auseinandergesetzt hatte und ob sich das TMIK vom TLfDI zu einer solchen Software hatte beraten lassen. Das TMIK bat den TLfDI um eine Zuarbeit. Hier konnte der TLfDI dem TMIK mitteilen, dass auf eine Anfrage des TLfDI im Januar 2018 an das TMIK dieses im Februar 2018 erklärte, dass die Thüringer Polizei Software für Vorhersagemodelle für Straftaten zur damaligen Zeit weder einsetzte noch plante.
Zugleich wies der TLfDI im Rahmen seiner Zuarbeit an das TMIK darauf hin, dass im Rahmen der Veranstaltung des TLfDI zum Thema „Trojaner, Body-Cams und Co. – Polizeiarbeit zwischen Sicherheit und Schutz der informationellen Selbstbestimmung“ am 18. Januar 2018 Herr Prof. Dr. Dirk Labudde mit seinem Vortrag „Predictive Policing – gestern, heute, morgen“ zu diesem Thema referierte.

3.4 „Wer zeigt hier wen an?“ – Anzeigenaufnahme bei der Thüringer Polizei

Anzeigen bei der Thüringer Polizei werden nur in einem separaten Raum ohne Beisein Dritter aufgenommen, sofern sich aus einer Erstbefragung des Anzeigeerstatters ein Straftatverdacht ergibt. Soweit zeitgleich mehrere Anzeigen innerhalb einer Polizeidienststelle aufge-

geben werden, ist die Geheimhaltung personenbezogener Daten zu gewährleisten.

Ein Bürger wandte sich gemäß § 8 Abs. 1 Thüringer Datenschutzgesetz an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Gemäß dieser Norm kann sich jede betroffene Person, unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs, mit einer Beschwerde unmittelbar an den TLfDI wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen des Landes in ihren Rechten verletzt worden zu sein.
Der Beschwerdeführer teilte dem TLfDI mit, dass er bei einer Polizeiinspektion eine Anzeige aufgegeben hatte. Dabei hatte der Beamte im Beisein einer weiteren Person die Personalien aus dem Personalausweis des Beschwerdeführers aufgenommen und dessen Anliegen abgefragt. Außerdem war der Beschwerdeführer Zeuge geworden, wie eine andere Person im Besucherraum eine Anzeige aufgegeben hat.
Nach eingehender Stellungnahme durch die betreffende Polizeiinspektion sowie datenschutzrechtlicher Würdigung konnte der TLfDI den Sachverhalt schnell aufklären. In der besagten Polizeiinspektion existiert ein Besucherraum, in den die Bürgerinnen und Bürger begleitet werden können. Dieser Raum ist vom Eingangs- beziehungsweise Empfangsbereich separiert und eine Befragung erfolgt dort ausschließlich ohne dritte Personen. Jedoch befindet sich dieser Raum bereits im Sicherheitsbereich der Dienststelle, sodass im Vorfeld eine Dokumentation jeder betroffenen Person, die den Sicherheitsbereich betritt, mittels Identitätsdokument erfolgen muss, auch weil ihr ein Besucherausweis ausgehändigt wird.
Die Nachfrage des TLfDI bei der zuständigen Polizeidienststelle ergab, dass es sich im vom Beschwerdeführer geschilderten Falle nicht um eine Anzeigenaufnahme, sondern um eine solche typische Vorbereitungsmaßnahme im Zugangs-/Bürgerbereich der Polizeiinspektion handelte. Hierzu gehört neben der Identitätsfeststellung die informatorische Befragung. Die einschlägigen Rechtsgrundlagen für eine solche Befragung finden sich – je nach Sachlage – in § 13 Thüringer Polizeiaufgabengesetz beziehungsweise in §§ 163 und 163b Abs. 2 Strafprozessordnung. Im Zuge der informatorischen Befragung sind die Beamtinnen und Beamten gehalten, den Grundsachverhalt zu erfragen, um dann über weitere Maßnahmen entscheiden zu können. Sofern sich aus dieser Erstbefragung ein Straftatverdacht ergibt und

eine Anzeigenaufnahme auf der Dienststelle notwendig wird, erfolgt diese in einem separaten Raum (Besucherraum) ohne Beisein Dritter. Nach Angaben der Polizeidienststelle wurden im zu Grunde liegenden Fall mangels Anfangsverdachts einer Straftat oder Ordnungswidrigkeit polizeilicherseits keine weiteren Maßnahmen veranlasst. Insofern konnte durch den gesprächsführenden Beamten keine Anzeige aufgenommen werden. Demnach war eine Separierung durch die gesprächsführenden Beamten auch nicht angezeigt.
Bezüglich der „mitgehörten Anzeigenaufnahme“ räumte die vom TLfDI befragte Polizeiinspektion aber ein, dass der gesprächsführende Beamte tatsächlich einer Anzeigeerstatterin beim Ausfüllen der schriftlichen Anzeige behilflich war, welche diese mangels anderer räumlicher Optionen im Warteraum ausfüllte. Insoweit konstatierte die Polizeiinspektion, dass aufgrund der andauernden Corona-Pandemielage und zur Einhaltung des Behördenschutzkonzepts der Polizei die Bediensteten angehalten waren, grundsätzlich möglichst viele geeignete Fälle auf schriftlichem Weg aufzunehmen beziehungsweise anzeigen zu lassen. Von daher sei es, so die Polizeidienststelle in ihrer Stellungnahme gegenüber dem TLfDI, umso notwendiger gewesen, konkrete Erkenntnisse zu dem zu Grunde liegenden Sachverhalt zu erfragen. Dafür sei nicht in allen Fällen eine Separierung der Bürgerinnen und Bürger möglich gewesen. Dabei räumte die Polizeiinspektion ferner ein, dass dadurch eine „Geheimhaltung persönlicher Anliegen", wie vom Beschwerdeführer bemängelt, zumindest im Rahmen der Erstbefragung nicht durchgehend möglich gewesen sei.
Der Vorfall wurde vom TLfDI zum Anlass genommen, die Dienststellen und Organisationseinheiten der Thüringer Polizei hinsichtlich der Geheimhaltung personenbezogener Daten zu sensibilisieren.

3.5 Neufassung der Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung

Bei der Erstellung von Verordnungen ist in Bezug auf die datenschutzrechtlichen Aspekte oft auch die Expertise des TLfDI gefragt. Das Thüringer Ministerium für Inneres und Kommunales bat aus diesem Grund den TLfDI zur Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung um eine datenschutzrechtliche Stellungnahme.

Die rechtlichen Grundlagen für Datenverarbeitungen bei der Thüringer Polizei werden im Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (PAG) und im Thüringer Datenschutzgesetz festgelegt.
Zur Erfüllung der Aufgaben der Polizei werden rechtmäßig erlangte personenbezogene Daten dort zeitlich befristet gespeichert. Dennoch dürfen personenbezogene Daten nicht unendlich lang gespeichert werden. Daher wird sowohl im Einzelfall als auch nach festgelegten Fristen (Aussonderungsprüffristen) seitens der Polizei geprüft, ob die Voraussetzungen für eine Aufrechterhaltung der Speicherung noch vorliegen.
Im Berichtszeitraum passte das Thüringer Ministerium für Inneres und Kommunales (TMIK) die Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) an die Neuregelungen, die sich aus der Umsetzung der JI-Richtlinie ergaben und bereits 2018 in Thüringen mit einem geänderten Thüringer Datenschutzgesetz und geänderten Thüringer Polizeiaufgabengesetz (PAG) einhergingen, an.
Gemäß § 40 Abs. 7 PAG wird das TMIK ermächtigt, durch Rechtsverordnung weitere Kriterien für die Festlegung der Aussonderungsprüffristen zu regeln. Hierzu bat das Ministerium auch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Stellungnahme zu der geänderten Prüffristenverordnung.
Gemäß § 1 Abs. 3 des Entwurfs der ThürPolPrüffristVO sind die maßgeblichen Gründe für die Aufrechterhaltung der Speicherung personenbezogener Daten aktenkundig zu machen. Der TLfDI empfahl, dass die maßgeblichen Gründe dabei nicht nur aus einem Verweis auf eine Rechtsvorschrift bestehen sollten, sondern, dass immer nachvollziehbar schriftlich dokumentiert wird, aufgrund welcher konkreten Gründe die Aufrechterhaltung der Speicherung im Einzelfall vorgenommen wird.
Bezüglich § 3 ThürPolPrüffristVO riet der TLfDI anstatt des Begriffs Zustimmung den in § 40 Abs. 3 PAG verwendeten Begriff der Einwilligung zu verwenden, um eine Einheitlichkeit herzustellen und Missverständnisse zu vermeiden.
Abschließend bekräftigte der TLfDI auch noch einmal seine Kritik an der Systematik der Fristenberechnung – auch wenn diese nicht in der ThürPolPrüffristVO, sondern in § 40 Abs. 6 PAG geregelt ist. An seinen sachlichen Kritikpunkten an der Fristenberechnung (siehe dazu

den 10. Tätigkeitsbericht, Nr. 7.8 „Jungbrunnen“ für Prüf- und Löschfristen“ sowie den 11. Tätigkeitsbericht Nr. 7.11 „Prüf- und Löschfristen der Polizei – Fortsetzung folgt...“) hält der TLfDI nach wie vor fest. Soweit nämlich innerhalb der Speicherfrist eines Ereignisses (Straftat) ein neues Ereignis (Straftat) hinzukommt, beginnt die Prüffrist neu zu laufen. Dies hat zu Folge, dass auch die vergangenen Ereignisse nunmehr dieser neuen Speicherungsfrist unterliegen. Aus datenschutzrechtlicher Sicht ist diese Lösung unbefriedigend, da es immer wieder zu einer Art „Neustart“ der jeweiligen Prüffrist kommt. Vielmehr müsste für jedes einzelne Ereignis auch eine separate Prüffrist gelten. Dabei ist entscheidend, dass die Akten anlässlich der Einzelfallbearbeitung oder nach Ablauf der jeweiligen Prüffrist „in die Hand genommen werden“, eine Erforderlichkeitsprüfung durchgeführt wird und in diesem Zusammenhang entweder eine weitere Prüffrist (für das jeweilige Ereignis) festgelegt wird oder die Daten gelöscht beziehungsweise vor einer Aktenvernichtung dem Archiv angeboten werden.

3.6 Was hat der Gerichtsvollzieher zu tun – und darf ihn der TLfDI kontrollieren?

Die Gerichtsvollzieher sind zwar selbstständige Organe der Rechtspflege, aber keine eigenständigen Organisationseinheiten der Landesjustizverwaltung. Sie gehören den Amtsgerichten an und unterstehen der Dienstaufsicht des Direktors. Nach § 22 Satz 1 GVGA verschließt der Gerichtsvollzieher bei jeder Zustellung, die durch Übergabe an einen Ersatzempfänger, durch Niederlegung oder durch Einlegen in den Briefkasten oder eine ähnliche Vorrichtung geschieht, das zu übergebende Schriftstück in einem Umschlag.

Im Berichtszeitraum erreichten den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mehrere Beschwerden über das Vollstreckungsvorgehen von Gerichtsvollziehern. Insbesondere rügten die Beschwerdeführer die offene Zustellung ohne Briefumschläge, insbesondere von Pfändungs- und Überweisungsbeschlüssen an dritte Personen und nicht an den Schuldner selbst.
Zunächst war bei diesen Fällen im Justizbereich die Frage zu klären, ob die einzelnen Verarbeitungsvorgänge der Gerichtsvollzieher, gegen die sich die Beschwerdeführer wandten, als justizielle Tätigkeit einzustufen waren. Wenn ein Fall als justizielle Tätigkeit einzustufen

ist, hat dies zur Folge, dass der TLfDI als Aufsichtsbehörde nicht zuständig ist. Art. 55 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) und Art. 45 Abs. 2 der JI-Richtlinie enthalten Bestimmungen, wonach die Aufsichtsbehörden nicht für die Aufsicht über Verarbeitungen zuständig sind, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen. Zusätzlich findet sich in § 2 Abs. 9 Thüringer Datenschutzgesetz (ThürDSG) die Regelung, dass für die Gerichte und Stellen des Justizbereichs die Vorschriften dieses Teils nur gelten, soweit sie Verwaltungsaufgaben wahrnehmen.

Zur Erfüllung der gerichtlichen Aufgaben im Rahmen der justiziellen Tätigkeit zählen nicht nur jene des Richters, sondern alle Aufgaben, die aufgrund der gesetzlichen Regelungen im Gerichtsverfassungs- und Prozessrecht durch die Organe der Rechtspflege innerhalb der verfassungsrechtlich garantierten Unabhängigkeit bei der Durchführung eines gerichtlichen Verfahrens erfüllt werden.

Damit fallen in die Kontrollzuständigkeit des TLfDI einerseits klassische Verwaltungsaufgaben der Gerichte (beispielsweise Beschaffung, Personalsachen et cetera) und andererseits Justizverwaltungshandeln. Nicht der Kontrollzuständigkeit des TLfDI unterliegen sämtliche Tätigkeiten des Gerichts im Zusammenhang mit einem laufenden gerichtlichen Verfahren, die auf die Beendigung des Verfahrens gerichtet sind beziehungsweise hierzu beitragen sollen (vergleiche Abgrenzung gemäß Bundesverfassungsgericht, Beschluss vom 2. Dezember 2014 – 1 BvR 3106/09: *„Dies gilt insbesondere dann, wenn die Mitteilung nicht der Entscheidung des Rechtsstreits oder der Streitbeilegung bzw. letztverbindlichen Klärung der Rechtslage in dem zugrundeliegenden Rechtsstreit dient*“).

Nach Ansicht des TLfDI gehören mit zur justiziellen Tätigkeit des Gerichts (und damit der Kontrolle des TLfDI entzogen) solche Tätigkeiten der Geschäftsstelle eines Gerichts, in denen sie bei der Bearbeitung von laufenden Gerichtsverfahren als „verlängerter“ Arm des entscheidenden Gerichts (Einzelrichter/in oder Spruchkörper) bei solchen Handlungen tätig wird, die auf die Beendigung des Rechtsstreits gerichtet sind. Dies gilt unabhängig davon, ob die Geschäftsstelle aufgrund einer konkreten Einzelanweisung des zuständigen Gerichts handelt oder aufgrund einer Generalanweisung, in entsprechenden Fällen stets derart zu verfahren. Alle übrigen Tätigkeiten der Geschäftsstelle werden mithin als Verwaltungstätigkeit eingestuft.

Damit unterfallen nach Ansicht des TLfDI die Gerichtsvollzieher auch unter dessen Kontrollzuständigkeit, weil sie nicht selbst „das Gericht“

sind und nicht als „verlängerter Arm“ des entscheidenden Gerichts tätig werden. Die Gerichtsvollzieher sind zwar selbstständige Organe der Rechtspflege, aber keine eigenständigen Organisationseinheiten der Landesjustizverwaltung. Sie gehören den Amtsgerichten an und unterstehen der Dienstaufsicht des Direktors, sofern es sich nicht um ein Arbeitgeberverhältnis des Gerichtsvollziehers zu einer von ihm eingestellten Bürokraft handelt. Zudem dürfen sie auch keine (unabhängige) justizielle Tätigkeit ausführen (vergleiche Bundesverwaltungsgericht (BVerwG) Urteil vom 29. April 1982 – 2 C 33/80 -, BVerwGE 65, 260-270).
Gleiches gilt für die Staatsanwaltschaften und deren Geschäftsstellen.
Nachdem nun die Verarbeitungsvorgänge der Gerichtsvollzieher in den Kontrollbereich des TLfDI fallen, war nunmehr vom TLfDI zu klären, ob eine offene Zustellung ohne Umschlag von Drittschuldnererklärungen datenschutzrechtlich zulässig war. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden, das heißt, die personenbezogenen Daten müssen auf einer zulässigen Rechtsgrundlage und in rechtmäßiger Weise verarbeitet werden. Dafür müssen bei der Verarbeitung auch alle zusätzlichen Anforderungen und Pflichten beachtet werden, die sich aus der DS-GVO oder aus dem nach der DS-GVO zulässigen nationalen Recht ergeben, also hier dem nachfolgenden § 22 Geschäftsanweisung für Gerichtsvollzieher (GVGA) entsprechen.
Nach § 22 Satz 1 GVGA verschließt der Gerichtsvollzieher bei jeder Zustellung, die durch Übergabe an einen Ersatzempfänger, durch Niederlegung oder durch Einlegen in den Briefkasten oder eine ähnliche Vorrichtung geschieht, das zu übergebende Schriftstück in einem Umschlag, nachdem er auf dem Umschlag das Datum, die Dienstregisternummer und gegebenenfalls die Uhrzeit der Zustellung vermerkt und den Vermerk unterschrieben hat. Nach § 22 Satz 2 GVGA ist das Schriftstück so zu verschließen, dass es ohne Öffnung nicht eingesehen werden kann. Die Außenseite des Briefumschlags ist mit dem Namen und der Amtsbezeichnung des Gerichtsvollziehers sowie mit dem Namen des Zustellungsadressaten zu versehen, vergleiche § 22 Satz 2 GVGA. Schließlich weist der Gerichtsvollzieher nach § 22 Satz 2 GVGA den Ersatzempfänger darauf hin, dass er verpflichtet ist, die Schriftstücke dem Zustellungsadressaten alsbald auszuhändigen.
Gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich

Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“) bietet. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gemäß Art. 32 Abs. 1 Buchstabe b) DS-GVO die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, ein.
Bei einer offenen Übermittlung ist grundsätzlich die Vertraulichkeit gefährdet, da die Gefahr besteht, dass unbefugte Personen einen Zugriff auf die personenbezogenen Daten erhalten können. In den dem TLfDI vorliegenden Fällen wurden die Pfändungs- und Überweisungsbeschlüsse offen, ohne Briefumschlag, an dritte Personen, unter anderem angestellte Mitarbeiter, übergeben. Eine Vertraulichkeit der personenbezogenen Daten war in diesen Fällen somit nicht gegeben. Der TLfDI beabsichtigt daher, in den genannten Fällen eine Verwarnung zu erlassen, wenn die Sachlage abschließend geklärt ist. Über die Ergebnisse wird der TLfDI im nächsten Tätigkeitsbericht berichten.

3.7 Sechstes Gesetz zur Änderung der Thüringer Kommunalordnung – Anhörungsverfahren vor dem Thüringer Landtag

Im Rahmen des Anhörungsverfahrens hatte der TLfDI die Gelegenheit, zu den geplanten Regelungen Stellung zu nehmen. Da teils weitreichende datenschutzrechtliche sowie -technische Aspekte betroffen waren, wie etwa die Videoübertragung von Sitzungen, unterbreitete der TLfDI dem Thüringer Landtag Verbesserungsvorschläge für eine datenschutzkonforme ThürKO.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde gemäß §§ 79 und 112 Abs. 4 der Ge-

schäftsordnung des Thüringer Landtags zum Sechsten Gesetz zur Änderung der Thüringer Kommunalordnung (ThürKO) angehört, nachdem in der ersten Beratung des Thüringer Landtags beschlossen wurde, das Änderungsgesetz an den Innen- und Kommunalausschuss zu verweisen, der eine schriftliche Anhörung beschloss.
Im Rahmen der schriftlichen Anhörung nahm der TLfDI neben dem Gesetzentwurf der Fraktionen DIE LINKE, der SPD und Bündnis 90/DIE GRÜNEN vom 8. Juli 2020 (Drucksache 7/1188 – nachfolgend ThürKO-E-Regierung) auch zu dem Gesetzentwurf der Fraktion der FDP vom 22. April 2020 (Drucksache 7/651 – nachfolgend ThürKO-E-FDP) und dem Gesetzentwurf der Fraktion der CDU vom 3. Juni 2020 (Drucksache 7/869 – nachfolgend ThürKO-E-CDU) Stellung; die Drucksachen sind abrufbar unter: https://parldok.thueringen.de/ParlDok.
Insbesondere der Gesetzentwurf der Fraktion der FDP sowie jener der Fraktion der CDU enthielten die dringend benötigten Rechtsvorschriften für das digitale Zeitalter. Dass die ThürKO einer Novellierung diesbezüglich bedarf, hatten zuletzt die Corona-Pandemie und die daraus resultierenden Einschränkungen sowie Auswirkungen aufgezeigt. Viele Kommunen hatten sich die Frage gestellt, ob es datenschutzrechtlich sowie -technisch zulässig ist, digitale Ratssitzungen unter anderem per Livestream abzuhalten. Die ThürKO in der derzeitigen Fassung enthält hierzu keine konkrete Regelung. Der TLfDI sah daher die Chance, mit dem Sechsten Änderungsgesetz zur ThürKO verbindliche Regelungen zu schaffen, damit die Kommunen in diesem Punkt Rechtsklarheit aus datenschutzrechtlicher sowie -technischer Sicht haben.
Im Rahmen der Anhörung hat der TLfDI dem Thüringer Landtag zahlreiche Verbesserungsvorschläge zu den einzelnen Gesetzentwürfen unterbreitet, unter anderem zur beabsichtigten Ausweitung der Saalöffentlichkeit sowie zu den Informations- und Beteiligungsrechten der Einwohner, Kommunalvertretungen und ihrer Mitglieder. Besonderen Nachholungsbedarf sah der TLfDI bei den folgenden Aspekten:

– **Einsatz von Videokonferenzsystemen:**

Der TLfDI begrüßte grundsätzlich die Aufnahme einer Regelung, die es gestattet, in Ausnahmefällen Gemeinderatssitzungen im Wege einer Telefon- oder Videokonferenz abzuhalten. Er wies jedoch darauf hin, dass bei der Wahl der Videokonferenzsysteme darauf zu achten sei, dass die verantwortlichen Betreiber der Videokonferenzsysteme dem Anwendungsbereich der Datenschutz-Grundverordnung (DS-

GVO) unterliegen. Welches Videokonferenzsystem zum Einsatz kommt und wer der Verantwortliche gemäß Art. 24 DS-GVO ist, sei vorab schriftlich festzulegen. Auch bedürfe es noch solcher Regelungen zu Ton- und Videoaufzeichnungen, durch die die an der Videokonferenz teilnehmenden Gemeinderatsmitglieder selbst die Mitschnitte mit ihren personenbezogenen Daten erlauben oder untersagen.
(§ 36 Abs. 4 ThürKO-E-FDP sowie § 39 Abs. 1 ThürKO-E-CDU).

– **Ausweitung der Saalöffentlichkeit:**

Der TLfDI begrüßte ebenfalls die Aufnahme einer Norm, die die Ausweitung der so genannten Saalöffentlichkeit hin zur Medienöffentlichkeit regelt (Saalöffentlichkeit bedeutet, dass sich jedermann Kenntnis von Ort und Zeit der Sitzung verschaffen kann und im Rahmen der tatsächlichen Gegebenheiten auch Zutritt erhalten muss). Denn der TLfDI hatte bereits mehrfach in der Vergangenheit die Implementierung einer Regelung in § 40 ThürKO angeregt, die die Zulässigkeit von Bild-, Film- und Tonaufnahmen durch die Gemeinde in öffentlichen Sitzungen des Gemeinderats sowie deren Veröffentlichungen in Telemedien regelt. Der TLfDI hatte deshalb erneut einen Regelungsvorschlag unterbreitet, um eine datenschutzkonforme Regelung zu gewährleisten, die den Kommunen jegliche Rechtsunklarheit nimmt, da die Entwürfe in den zu beurteilenden Gesetzentwürfen Schwachstellen aufwiesen.
(§ 40a ThürKO-E-FDP sowie § 40 Abs. 3 und 4 ThürKO-E-CDU).

– **Einwohnerfragestunde:**

Verbesserungsbedarf erkannte der TLfDI auch bei dem Regelungsentwurf zur Einwohnerfragestunde. Sollte es sich abzeichnen, dass persönliche Angelegenheiten mit personenbezogenen Daten Dritter vorgebracht werden, so müsste dies gegebenenfalls fallbezogen in die nicht öffentliche Sitzung „verschoben“ werden. Zudem ist darauf zu achten, dass bei der Beantwortung der Fragen keine personenbezogenen Daten offenbart werden, wenn die Interessen Einzelner entgegenstehen.
(§ 15 Abs. 1a ThürKO-E-Regierung).

– **Abschriften von Niederschriften nicht öffentlicher Sitzungen:**

Der TLfDI lehnte die geplante Änderung ab, die beinhaltete, dass die Mitglieder neben den Niederschriften der öffentlichen Sitzungen auch Abschriften anfertigen können von den Niederschriften der nicht öffentlichen Sitzungen. Dies ist aus datenschutzrechtlicher Sicht äußerst

problematisch, insbesondere dann, wenn die Abschriften der nicht öffentlichen Sitzungen zur Lektüre mit nach Hause genommen werden. Nicht nur der TLfDI sah darin eine erhebliche Gefahr, sondern auch die herrschende Meinung in der Kommentarliteratur.
(§ 42 Abs. 3 Satz 1 und 2 ThürKO-E-Regierung).
Inwieweit die Verbesserungsvorschläge des TLfDI berücksichtigt werden, bleibt noch abzuwarten, da sich das sechste Gesetz zur Änderung der ThürKO zum Zeitpunkt der Erstellung dieses Tätigkeitsberichtes noch in der nicht öffentlichen Ausschussberatung des Innen- und Kommunalausschusses befand (Stand: 29. Januar 2021).
Der Verlauf des Änderungsgesetzes ist in der Parlamentsdokumentation des Thüringer Landtags einsehbar unter: http://www.parldok.thueringen.de/ParlDok/vorgaenge/76339/1. Zudem ist die Stellungnahme des TLfDI zum sechsten Gesetz zur Änderung der ThürKO abrufbar unter: https://beteiligtentransparenzdokumentation.thueringer-landtag.de/fileadmin/Redaktion/Beteiligtentransparenzdokumentation/Dokumente/7-1188/3_Parl_Anhoerungsverf/V7-919/V7-919.pdf.

3.8 Fehlerhaftes Update: Offenlegung von Kundendaten in einer Stadtbücherei

Bei der Installation von Softwareupdates sowie der Änderung von E-Mail-Vorlagen sollte darauf geachtet werden, dass diese vorab in einer Testumgebung getestet werden. Durch das Überprüfen von neuen und geänderten Inhalten vor der Inbetriebnahme lassen sich häufig Verletzungen des Schutzes personenbezogener Daten vermeiden.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von einer Stadtverwaltung gemeldet, dass die Namen und Kundennummern von Nutzern einer Stadtbücherei per E-Mail an andere Nutzer versandt worden waren. Im Rahmen der Überprüfung der Meldung der Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Datenschutz-Grundverordnung (DS-GVO) stellte sich heraus, dass aufgrund eines Softwareupdates eine angepasste E-Mail-Vorlage durch eine Standard-Vorlage ersetzt worden war. Ein Mitarbeiter der Stadtbücherei wollte den alten Zustand wiederherstellen und änderte die Vorlage. Allerdings unterlief ihm ein Fehler, was letztlich zu einem Versand von E-Mails mit fehlerhaften Inhalten führte.

Um die daraus entstandene Verletzung des Schutzes personenbezogener Daten abmildern zu können, informierte die Stadtbücherei die betroffenen Personen gemäß Art. 34 DS-GVO mit dem Hinweis, dass die Möglichkeit der Vergabe einer neuen Kundennummer besteht. Zusätzlich wurden alle Empfänger der falschen E-Mails aufgefordert, diese zu löschen.
Um die Ursache für den fehlerhaften Versand zu beheben, veranlasste die Stadtbücherei die Nachinstallation eines Backups.
Die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen wurden vom TLfDI als ausreichend und angemessen erachtet. Der TLfDI empfahl – auch als Konsequenz aus dieser Datenpanne – ferner, dass Updates an der Software und auch Änderungen an E-Mail-Vorlagen vorab in einer Testumgebung getestet werden, um Verletzungen des Schutzes personenbezogener Daten im Vorfeld vermeiden zu können.

3.9 Umfrage zur Veröffentlichung von Jubiläen im Amtsblatt

Auch wenn es einige kommunale Würdenträgerinnen und Würdenträger nicht gern hören: Die Veröffentlichung von Altersjubiläen und hohen Geburtstagen gemäß § 50 Abs. 2 Bundesmeldegesetz (BMG) ist nur nach vorheriger Einwilligung des Jubilars/ der Jubilarin zulässig. Denn das Amtsblatt der Kommune fällt nicht unter den Begriff der Presse im Sinne der genannten Norm. Wenn also ein Bürgermeister/ eine Bürgermeisterin die hohen Geburtstage oder Ehejubiläen in seinem/ ihrem Amtsblatt veröffentlichen möchte, muss er/ sie vorher die Einwilligung des Jubilars/ der Jubilarin zu diesem Zweck einholen.

Ein datenschutzrechtlicher „Dauerbrenner“, der immer wieder Kommunen, Amtsleiterinnen und Amtsleiter sowie Bürgermeisterinnen und Bürgermeister beschäftigt, ist die Frage, ob und auf welcher Rechtsgrundlage personenbezogene Daten der Einwohnerinnen und Einwohner von den Meldebehörden an die Redaktion des Amtsblattes des Kommune zum Zweck der Gratulation zu hohen Geburtstagen oder Ehejubiläen übermittelt werden dürfen.
Ausgangslage für dieses Problem ist dabei der Regelungsgehalt von § 50 Abs. 2 Bundesmeldegesetz (BMG), der da lautet:
„(2) Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über

1. Familienname,
2. Vornamen,
3. Doktorgrad,
4. Anschrift sowie
5. Datum und Art des Jubiläums.
Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum."

Um sich einerseits ein Bild von der tatsächlichen Situation in Thüringer Kommunen zu dieser Problematik zu machen und zum anderen um den Verantwortlichen in Thüringer Rathäusern und Landratsämtern Hilfestellungen an die Hand zu geben, startete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits im Herbst 2019 eine anonymisierte Umfrageaktion in Thüringer Kommunen. Der TLfDI erfragte mittels eines kurzen Fragebogens unter anderem, auf welcher Rechtsgrundlage die Kommunen die Veröffentlichung der personenbezogenen Daten hoher Geburtstage und Ehejubiläen vornehmen und beabsichtigen, solche vorzunehmen oder, ob diese Veröffentlichung auf der Grundlage einer von Zeit zu Zeit aktualisierten Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO erfolge. Ferner fragte der TLfDI, ob bei den Kommunen das Bedürfnis für eine solche Muster-Einwilligung zur Veröffentlichung hoher Geburtstage und Altersjubiläen im Amtsblatt bestehe.

Die Auswertung dieser Umfrage erfolgte danach beim TLfDI im ersten Quartal des Berichtszeitraumes. Die Auswertung ergab folgendes „Lagebild":

Mit 112 Antworten war die Umfrage für den TLfDI im hohen Maße geeignet, sich einen Überblick über die Situation in den Kommunen zu vermitteln.

Dabei zeigte sich, dass jeweils die Hälfte der an der Umfrage teilnehmenden Kommunen die Veröffentlichung von Jubiläen und Geburtstagen in Amtsblättern weiterhin plant oder dies jedenfalls für die Zukunft nicht ausschließt, während die andere Hälfte eine solche Veröffentlichung nicht plant.

Unsicherheiten fielen bei der Rechtsgrundlage und insbesondere der rechtskonformen Umsetzung auf. So gingen zehn der befragten Kommunen entgegen der Ansicht des TLfDI davon aus, dass eine Veröffentlichung auch ohne Einwilligung der Jubilare möglich sei. Soweit

dafür als Begründung auf eine langjährige Verwaltungspraxis verwiesen worden ist, weist der TLfDI darauf hin, dass sowohl im Meldewesen durch Übergang der Kompetenz auf den Bund als auch im Datenschutz in den letzten Jahren erhebliche Änderungen der Rechtslage zu berücksichtigen sind (die nachfolgend auch noch einmal dargestellt werden). Landesrechtliche Regelungen hierzu sind bundesweit in einer Vielzahl entfallen und werden durch das geltende Bundesmeldegesetz nicht vollständig ersetzt.
Insgesamt hielt eine knappe Mehrheit der teilnehmenden Kommunen zudem die Erstellung einer Mustervorlage für die Einwilligung durch den TLfDI für eine sinnvolle Maßnahme.
Aus der weiteren Auswertung der Umfrage ergab sich aus Sicht des TLfDI, die Rechtslage zu der Problematik noch einmal Schritt für Schritt zu erläutern:
Aus rechtlicher Sicht sind bei der Gratulation zu Jubiläen und hohen Geburtstagen durch Amtsträger drei Schritte streng zu trennen:
1. Die Anfrage der Kommune bei und Mitteilung der Jubiläen und Geburtstage durch die Meldebehörde (zulässig gemäß § 50 Abs. 2 Satz 2 BMG),
2. Die Gratulation durch den Mandatsträger und dafür notwendige Datenverarbeitungen innerhalb der Kommune (zulässig gemäß § 16 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG)),
3. Eine Veröffentlichung im kommunalen Amtsblatt oder auf anderem Wege (grundsätzlich unzulässig, aber auf Basis einer Einwilligung möglich).
Zu (1.): Die Anfrage der Kommune bei der Meldebehörde und die Mitteilung von Jubiläen und Geburtstagen durch diese stellt sich zunächst weitgehend unproblematisch dar. Dies ergibt sich aus § 37 Abs. 1 und § 34 Abs. 1 in Verbindung mit § 50 Abs. 2 BMG. Die Bürgermeister der Kommunen sind insoweit Mandatsträger im Sinne dieser Vorschrift und können die dort im Einzelnen aufgezählten Daten von der Meldebehörde erhalten, soweit dem nicht gemäß § 50 Abs. 5 BMG widersprochen wurde. Dies hat die Meldebehörde zu prüfen. Meldebehörde ist zwar in Thüringen auch die Gemeinde (§ 1 BMG in Verbindung mit § 1 Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes), deren Arbeit aber intern von den sonstigen Teilen der Gemeindeverwaltung nach dem Prinzip der „informationellen Gewaltenteilung“ (Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 206 – Volkszählungsurteil) strikt zu trennen ist. Auf das Recht des § 50 Abs. 5 BMG ist regelmäßig und

ortsüblich durch die Meldebehörde hinzuweisen, damit die Betroffenen hiervon Kenntnis erlangen.
Nicht explizit geregelt ist in § 50 Abs. 2 BMG die Erlaubnis des Mandatsträgers, diese Anfrage auch zu stellen. Denn das BMG richtet sich ausschließlich an die Meldebehörden. Die Norm ist jedoch Indiz für das Bestehen eines solchen Rechts, und das Interesse an der Übermittlung von Glückwünschen durch Persönlichkeiten des öffentlichen Lebens ist vom Gesetzgeber in den Materialen zum Melderecht ausdrücklich anerkannt (vergleiche Bundestags-Drucksache 17/7746, S. 46 zum BMG mit Verweis auf Bundestags-Drucksache 8/3825, S. 25 zum damaligen Melderechtsrahmengesetz).
Zu (2.): Nach der Anfrage ist regelmäßig zum Zwecke der späteren Gratulation eine Speicherung und weitere Verarbeitung der von der Meldebehörde empfangenen personenbezogenen Daten notwendig. Diese ist im Hinblick auf die oben beschriebene Anerkennung der Gratulationen in Verbindung mit § 16 Abs. 1 ThürDSG ebenfalls als zulässig einzustufen. Die Gratulation durch den Bürgermeister lässt sich somit als kommunale Selbstverwaltungsaufgabe einstufen. Ein ausreichender Bezug zu Gemeindebevölkerung oder Gemeindegebiet liegt hierfür vor. Dies gilt trotz des Wegfalls der Formulierung „zur Ehrung“ in § 33 Abs. 2 des früheren Thüringer Meldegesetzes (ThürMeldG – außer Kraft) auch weiterhin.
Zu (3.): Keine generelle Erlaubnis besteht jedoch zur Veröffentlichung der aus dem Melderegister erlangten personenbezogenen Daten der Jubilare. Die Veröffentlichung in einem Amtsblatt stellt einen zusätzlichen, vom BMG weder angesprochenen noch sinngemäß erfassten Verarbeitungsschritt dar. Die Veröffentlichung ist ein weiterer Arbeitsschritt, der auch nicht in die Kompetenz des Bundesgesetzgebers für das Melderecht fällt. Die Veröffentlichung ist dabei auch nicht ohne Weiteres als ungefährlich oder gar gewünscht einzustufen. Eine landesrechtliche Erlaubnis der Veröffentlichung ist nicht ersichtlich. Die kommunale Selbstverwaltung ist diesbezüglich im Hinblick auf das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz in seiner Ausprägung als Recht auf informationelle Selbstbestimmung begrenzt. Zum geeigneten Interessenausgleich ist es geboten, auf eine Veröffentlichung ohne Einwilligung des Betroffenen zu verzichten.
Insbesondere ist darauf hinzuweisen, dass das Amtsblatt einer Kommune nicht als Presseerzeugnis angesehen werden kann und sich die Veröffentlichungserlaubnis somit nicht aus presserechtlichen Erwä-

gungen und Abwägungen eines gegebenenfalls bestehenden öffentlichen Interesses ergeben kann. Den Gemeinden ist presseähnliche Betätigung gänzlich untersagt. Ist ein Amtsblatt presseähnlich, so führt dies keinesfalls zu erweiterten Veröffentlichungserlaubnissen, sondern die Veröffentlichung wäre insgesamt unzulässig (siehe beispielsweise zuletzt Bundesgerichtshof, Urteil vom 20. Dezember 2018 – I ZR 112/17).

Das Alter einer Person – wenn dies auch kein besonderes personenbezogenes Datum im Sinne des Art. 9 DS-GVO ist – gehört aufgrund der Anknüpfung von Diskriminierungen (siehe nur § 1 Allgemeines Gleichbehandlungsgesetz) an dieses Merkmal zu den besonders problematischen Datenkategorien. Durch die Bekanntgabe an eine breite Öffentlichkeit im Amtsblatt stellt sich diese Art der Verarbeitung zudem im Verhältnis zur Gratulation durch den Amtsträger als erheblicher Eingriff dar.

Im Hinblick auf aktuelle Kriminalstatistiken darf sicher auch die Problematik des so genannten Enkeltrick-Betrugs hier nicht gänzlich außer Acht gelassen werden. Eine Zweckentfremdung der grundsätzlich frei zugänglichen Amtsblätter scheint hier nicht gänzlich fernliegend, liefern die Informationen über das Alter der betroffenen Person hinaus sogar noch einen persönlichen Anknüpfungspunkt für die Kontaktaufnahme.

Verwaltungspraktisch ist auch folgende Überlegung anzustellen: Sicher ist nicht abzustreiten, dass viele Gemeindeangehörige sich über eine solche Ehrung freuen. Es ist aber an dieser Stelle auch darauf hinzuweisen, dass die Landesdatenschutzbeauftragten verschiedentlich auf eine nicht geringe Zahl von Anfragen und Beschwerden der Bürgerinnen und Bürger zu dieser Problematik verweisen. Zwar liegen hier in der Tat keine gesicherten statistischen Erkenntnisse vor, jedenfalls ist aber nicht pauschal davon auszugehen, dass jeder Bürger/ jede Bürgerin sich hierdurch geehrt fühlen wird. Gerade die Nennung des Alters stellt für einige Menschen doch ein sehr sensibles Thema dar. Einer nicht ganz irrelevanten Zahl von Bürgerinnen und Bürgern wird die Gratulation somit regelmäßig unrecht sein, sodass der damit verfolgte Zweck leider vollends verfehlt wird (vergleiche zu den sehr unterschiedlichen Reaktionen auf die Ehrung beispielsweise auch den 18. Tätigkeitsbericht des Sächsischen LfDI, Drucksache des sächsischen Landtags, 6/10549, S. 46, 48).

Einzig verbleibende Lösung mangels gesetzlicher Grundlage ist damit

die Einholung einer Einwilligung des geehrten Gemeindebürgers (Ausführlich dazu auch Lück/ Kenar, LKV 2019, 344).
Diese Überlegungen und Auswertungen seiner Umfrage zur Veröffentlichung von hohen Alters- und Ehejubiläen in Amtsblättern hat der TLfDI nach Ablauf des Berichtszeitraums dem Thüringer Gemeinde- und Städtebund sowie dem Thüringischen Landkreistag mitgeteilt. In diesem Schreiben war auch eine **Muster-Einwilligung** enthalten, die die Kommune berechtigt, personenbezogene Daten des Jubilars/ der Jubilarin für die Zwecke der Veröffentlichung hoher Alters- und Ehejubiläen in Amtsblättern zu verarbeiten.

3.10 Fehlversand von Mahnungen – auch ein Datenschutzproblem

Der Verantwortliche muss für die Datenverarbeitung von personenbezogenen Daten technische und organisatorische Maßnahmen nach dem Stand der Technik treffen, die die Sicherheit der Verarbeitung gewährleisten. Dazu gehört auch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen. Technik und Werkzeuge (= Tools) sind nur dann nützlich und unterstützend, wenn sie an der richtigen Stelle im notwendigen Umfang und mit menschlichem Augenmaß eingesetzt werden.

Es kommt durchaus vor, dass Kunden ihre Rechnungen nicht immer rechtzeitig zahlen. Den Unternehmen bleibt dann nichts anderes übrig, als Mahnungen zu versenden. Um sich Arbeit zu ersparen und möglichst effizient zu handeln, haben viele Unternehmen ihr Mahnwesen automatisiert. Leider kommt es auch bei automatisierten Verfahren wie auch bei menschlichem Handeln immer wieder zu Fehlern. So auch bei einer Energieversorgungsfirma, der dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitteilte, dass die Mahnungen unterschiedlicher Kunden zusammen in einem Briefumschlag versandt worden waren. Die betreffende Energieversorgungsfirma war dabei als öffentliche Stelle, die am Wettbewerb teilnimmt, gemäß § 26 Thüringer Datenschutzgesetz anzusehen. Hierbei handelte es sich um eine Meldung nach Art. 33 Datenschutz-Grundverordnung (DS-GVO). Danach müssen Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde diese unverzüglich und möglichst binnen

72 Stunden melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hiervon war nicht auszugehen, denn niemand möchte gerne, dass andere Personen erfahren, dass sie ihre Rechnungen nicht zahlen.
Grund für die Verletzung des Schutzes personenbezogener Daten war in diesem Fall, dass sich ein softwaretechnischer Fehler in die Reportgenerierung des Mahnlaufes eingeschlichen hatte. Somit war es den Empfängern, die diese Briefe erhielten, möglich, Einsicht in die Mahnungen anderer Kunden zu nehmen. Der Energieversorger war allerdings nicht untätig geblieben und ergriff sofort nach der Entdeckung des Fehlers Maßnahmen:
Um die daraus entstandene Verletzung des Schutzes personenbezogener Daten abmildern zu können, wurden die Verarbeitungsprozesse des Energieversorgers vorrübergehend bis zur Beseitigung des Fehlers gestoppt. Weiterhin wurden die Empfänger der fehlgesandten Schreiben identifiziert und aufgefordert, die fälschlicherweise erhaltenen Mahnschreiben mit einem beigefügten frankierten Rückumschlag zurückzusenden beziehungsweise die datenschutzkonforme Vernichtung zu bestätigen. Um das erneute Auftreten einer Fehlkuvertierung wirksamer ausschließen zu können, wurde ein moderneres Tool mit verbesserten Möglichkeiten der Dokumentensteuerung und -kontrolle eingeführt. Da die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Kunden führte, wurden die betroffenen Kunden von dem Energieversorger über die Verletzung ihrer personenbezogenen Daten benachrichtigt. Dazu ist der Verantwortliche nach Art. 34 Abs. 1 DS-GVO verpflichtet.
Der TLfDI konnte in seiner Prüfung feststellen, dass der Inhalt der Meldung den Anforderungen von Art. 33 DS-GVO entsprach, wonach eine Meldung zumindest folgende Informationen enthalten muss:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die vom Verantwortlichen ergriffenen und vorgeschlagenen Maßnahmen dienten der Abmilderung der aus dem Softwarefehler entstandenen nachteiligen Auswirkungen. Sie genügten der Aufarbeitung des Vorfalls mit dem Ziel, künftig ähnliche Vorfälle zu verhindern. Insbesondere wurden auch eine Plausibilitätsprüfung durchgeführt und Prüfroutinen eingeführt.
Der Verantwortliche wurde vorsorglich darauf hingewiesen, dass er dafür Sorge zu tragen hat, dass gemäß Art. 32 Abs. 1 Buchstabe d) DS-GVO „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ etabliert sein muss. Die technischen und organisatorischen Maßnahmen müssen sich dabei am „Stand der Technik“ (Art. 32 Abs. 1 Satz 1 DS-GVO) ausrichten.

3.11 (K)Ein Fall für kriminalistische Datenschützer: Patientenakten auf dem Friedhof

Im Fall einer „Datenpanne“ ist es hilfreich, wenn der Verantwortliche nachweislich alle organisatorischen und technischen Maßnahmen im Sinne von Art. 32 DS-GVO umgesetzt hat, um den Schutz von (Patienten-)Daten umfassend zu gewährleisten.

Ende Juni 2020 meldete ein Thüringer Klinikum dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Datenpanne der besonderen Art. Bei Aufräumarbeiten auf einem Friedhof wurden in einem Gebüsch Dokumente aus mehreren Patientenakten aufgefunden. Die Unterlagen waren ordentlich sortiert, mit Heftstreifen („Aktendullis“) zusammengeheftet und in eine Decke beziehungsweise ein Laken eingewickelt. Bei den Unterlagen handelte es sich um Stammdaten von Patienten (Name, Geburtsdatum et cetera), medizinische Befundunterlagen und Arztbriefe.
Im Rahmen eines Gesprächstermins und einer gemeinsamen Vor-Ort-Begehung von Mitarbeitern des TLfDI, der Klinikleitung und des Datenschutzbeauftragten des Klinikums erfuhr der TLfDI, dass sämtliche

aufgefundenen Unterlagen ursprünglich an das Klinikarchiv zur Aufnahme in die bereits dort befindlichen zugehörigen Patientenakten übergeben werden sollten. In der Form und Heftung, in der die Unterlagen auf dem Friedhof aufgefunden wurden, müssen sie sich ursprünglich auf der Station befunden haben, auf der die betroffenen Patienten sowohl stationär als auch ambulant behandelt worden waren. Von der Station sollten sie eigentlich durch das im Klinikum beschäftigte medizinische Personal ins Klinikarchiv, das sich im Keller des gleichen Gebäudes befindet, gebracht werden.
Behandlungsende für sämtliche aufgefundenen Aktenbestandteile der betroffenen Patienten war Juni/ Juli 2019. Nach diesem Zeitpunkt befand sich keiner der betroffenen Patienten nochmals zur Behandlung im Klinikum. Somit müssten sich die Akten ab Juni/ Juli 2019 bereits im Archiv befunden haben beziehungsweise auf dem Weg ins Archiv gewesen sein (Behandlungsstation, Postfächer und Archiv befinden sich im gleichen Gebäude). Sie konnten nur aus dem Postfach des medizinischen Personals auf der Behandlungsstation selbst und aus dem Postfach für das Patientenaktenarchiv im Kellerraum der Klinik abhandengekommen sein.
Aufgrund der Art der Aktenbestandteile und ihrer Auffindesituation war nicht von einem materiellen und/ oder kriminellen Hintergrund für das Entwenden der Aktenbestandteile auszugehen. Alle betroffenen Patienten wurden durch das Klinikum von dem Vorfall schriftlich gemäß Art. 34 Datenschutz-Grundverordnung (DS-GVO) informiert; zudem wurde ihnen vom Klinikum ein Gespräch angeboten.
Im Rahmen der Vor-Ort-Begehung mit Klinikleitung und Datenschutzbeauftragten erhielt der TLfDI ebenfalls umfassende Informationen über die technische und organisatorische Sicherung von Patientenunterlagen im Sinne von Art. 32 DS-GVO. Hierzu wurde im Rahmen der Begehung Folgendes festgestellt:
Ohne klinikeigene elektronische Zutrittskarte, die nur das Klinikpersonal besitzt, war es von außen nicht möglich, in den Kellerraum zu gelangen, in dem sich die Klinikpostfächer befinden. Innerhalb des Gebäudes waren sämtliche Zugänge zum Kellerraum der Klinikpostfächer gesichert, so dass ein Betreten über die inneren Klinikbereiche durch unbefugte dritte Personen und/ oder Patienten der Klink ebenfalls ausgeschlossen werden konnte.
Wenn die Behandlung der Patienten auf der Station beendet ist, wird die medizinische Dokumentation mit einem Arztbrief abgeschlossen und mit einem „Aktendulli“ zusammengeheftet. Sodann wird die ge-

heftete Dokumentation von einer Stationsschwester persönlich in das Archivpostfach im Keller des Klinikgebäudes gebracht. Dieses Postfach wird zweimal täglich durch die Archivarin geleert und die Dokumente der bereits im Archiv befindlichen Patientenakte zugefügt beziehungsweise, wenn dies der erste stationäre Aufenthalt des Patienten war, wird ein neuer (roter) Papp-Archiveinband um die Dokumente angebracht und die Akte ins Archiv aufgenommen.
Infolge der im Gespräch und im Rahmen der Vor-Ort-Begehung erlangten Informationen stellte der TLfDI aus datenschutzrechtlicher Sicht fest, dass im Rahmen des organisatorischen Ablaufs der Postverteilung und Übergang von Patientenakten beziehungsweise deren Bestandteilen ins Klinikarchiv keine technischen und/ oder organisatorischen Sicherheitsdefizite bestanden haben. Die Patienten der Station, von der die aufgefundenen Bestandteile der Patientenakten stammten, werden auch im Gebäude regelmäßig vom Klinikpersonal begleitet und hatten daher keine Zugriffsmöglichkeit.
Aufgrund sämtlicher Informationen aus dem Gespräch mit der Klinikleitung und der Vor-Ort-Begehung war nicht plausibel nachvollziehbar, an welcher Stelle beziehungsweise auf welchem Wege die aufgefundenen Aktenbestandteile entwendet werden konnten. Von einem kriminellen und/oder materiellen Hintergrund war bei der Entwendung der aufgefundenen Aktenbestandteile nicht auszugehen. Da die organisatorischen und technischen Schutzvorgaben nach Art. 32 DS-GVO ordnungsgemäß vorgegeben worden waren und sich der Sachverhalt nicht mehr weiter aufklären ließ, erschien die Verhängung eines Bußgeldes gegen das Klinikum nach Art. 83 DS-GVO nicht angezeigt.

3.12 Infektionsschutz kontra Datenschutz, Kopie ja oder nein – Nachweis der Masernschutzimpfung in Kindergarten und Schule

Für die Anfertigung und Speicherung einer Kopie des Impfausweises oder ärztlichen Attestes für die Schülerakte beziehungsweise zum Verbleib im Kindergarten besteht keine Rechtsgrundlage. Dies kann nur mit einer wirksamen Einwilligung der Eltern oder Sorgeberechtigten nach Art. 9 Abs. 2 Buchstabe a) DS-GVO erfolgen.

Mit Inkrafttreten des Masernschutzgesetzes im März 2020 erhielt der Thüringer Landesdesbeauftragte für den Datenschutz und die Infor-

mationsfreiheit (TLfDI) zahlreiche Beschwerden und Anfragen von Eltern, die den Umgang mit Impfdokumenten (Impfausweis oder ärztliches Attest über die Kontraindikation zur Impfung) von Kindern in Schulen und Kindergärten betrafen. Zentrale Fragen waren, ob Schulen und Kindergärten Kopien der Impfdokumente anfertigen und diese aufbewahren dürfen und wie die Nachweisführung zu erfolgen hat, wenn eine Masernimpfung aus medizinsicher Sicht kontraindiziert und insofern nicht erfolgt ist.

Nach § 20 Abs. 9 Satz 1 Infektionsschutzgesetz (IfSG) ist der Nachweis über die Masernschutzimpfung gegenüber der Leitung der jeweiligen Einrichtung zu erbringen. Der/die Leiter/in ist die Person, die mit den Leitungsaufgaben in der jeweiligen Einrichtung beauftragt ist, vergleiche § 2 Nr. 15 IfSG. Im Falle der Thüringer Schulen ist dies die Schulleitung, die in der Regel die jeweiligen Klassenlehrer mit der Entgegennahme des Impfnachweises beauftragt. Im Falle der Kindergärten ist dies der/ die Leiter/in des jeweiligen Kindergartens.

Eine Ausnahme von der Impfpflicht besteht unter anderem für Personen, die mit einem ärztlichen Attest nachweisen, dass eine Impfung aus gesundheitlichen Gründen kontraindiziert ist oder wenn die Personen bereits immun sind. Die medizinische Kontraindikation muss jedoch – ebenso wie der Nachweis über die erfolgte Impfung – ärztlich bestätigt sein, § 20 Abs. 9 Satz 1 Nummer 2 IfSG. Streitig war zunächst, ob dieses Zeugnis lediglich die Kontraindikation als solche bestätigen oder auch die Diagnose enthalten muss.

Im Oktober 2020 erfolgte eine Klärung dieser Fragen durch Änderung des von Schulen und Kindertagesstätten zu verwendendem Ankreuz-Formulars durch das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS). Nur dieses Formular ist zur Akte zu nehmen; wodurch bestätigt ist, dass keine Diagnosen oder Impfdokumente kopiert und zu den Akten genommen werden dürfen. Das neue Formular ist unter folgender Internetseite einsehbar: https://bildung.thuringen.de/fileadmin/schule/aktiv/gesundheit/Erfassungsbogen_Impfstatus_Masern_Schueler.pdf.

Ursprünglich, das heißt bis Oktober 2020, enthielt das Formular jedoch keine Ankreuzoption dafür, dass eine (ärztlich bestätigte) medizinische Kontraindikation für die Masernschutzimpfung vorliegt, wodurch die genannten Unklarheiten entstanden waren. Daher hatte sich der TLfDI bereits Anfang August 2020 schriftlich an das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie und das TMBJS gewandt und, um diese Lücke zu schließen, die Auf-

nahme einer entsprechenden Ankreuzoption für die Vorlage einer ärztlichen Kontraindikation empfohlen. In gegenseitiger Zusammenarbeit entstand sodann das aktuelle Formular.

3.13 Immer wieder die Frage: Was sind Sozialdaten?

Hierunter sind nur Daten zu verstehen, die den in § 35 Abs. 1 SGB I genannten Stellen in Eingrenzung des weit gefassten Wortlauts der Vorschrift im Zusammenhang mit einem Versicherungs- oder Sozialrechtsverhältnis, der Erbringung von Sozialleistungen oder diesen gleichgestellten Aufgaben bekanntgeworden sind.

Die Kassenärztliche Vereinigung fragte nach, ob auch Arztdaten, welche sie im Rahmen ihrer Aufgabenerfüllung erhebt und verarbeitet, als Sozialdaten zu qualifizieren sind. Hintergrund der Anfrage war ein staatsanwaltliches Auskunftsersuchen im Rahmen eines Ermittlungsverfahrens. Konkret ginge es hierbei um die Übermittlung des Arbeitsvertrages eines Arztes mit der Kassenärztlichen Vereinigung und Angaben über dessen Kontoverbindung, auf welche dessen Arbeitsentgelt überwiesen wurde. Unter Hinweis auf die Bestimmung des § 73 Sozialgesetzbuch Zehntes Buch (SGB X), nach dem für die Übermittlung von Sozialdaten an Strafverfolgungsbehörden ein richterlicher Beschluss erforderlich ist, hatten die Kassenärztliche Vereinigung zunächst die Auskunft verweigert und um Übersendung eines richterlichen Beschlusses gebeten.
Die Staatsanwaltschaft berief sich in der Folge auf einen Beschluss des Landgerichts Heidelberg vom 26. März 2004 mit dem Aktenzeichen 2 QS 26/04, wonach es keine sozialdatenschutzrechtliche Auskunftsbeschränkung in Bezug auf personenbezogene Daten der Ärzte gebe, da diese keine Sozialdaten darstellten, weil es sich hier nicht um Versicherten- oder Patientendaten handele. Danach stünden der Übermittlung an die Staatsanwaltschaft keine datenschutzrechtlichen Gründe entgegen.
Nach Prüfung der Rechtslage kam der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit zu folgendem Ergebnis:
Sozialdaten sind nach § 67 Abs. 2 SGB X personenbezogene Daten, die von einer in § 35 Abs. 1 Sozialgesetzbuch Erstes Buch (SGB I) gennannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeitet werden. Unzweifelhaft handelt es sich bei den an-

geforderten Daten um personenbezogene Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO). Der Begriff der „Aufgaben nach diesem Gesetzbuch“ wird, legt man den Regelungsgehalt des § 67 Abs. 3 SGB X zugrunde, sehr weit verstanden. Allerdings ist zu bedenken, dass zwar Träger des Geheimhaltungsanspruchs nach § 35 Abs. 1 SGB I grundsätzlich „jeder“ ist, nach dem Zweck der Vorschrift jedoch nur derjenige gemeint ist, dessen Daten den in § 35 Abs. 1 SGB I genannten Stellen im Zusammenhang mit einem Versicherungs- oder Sozialrechtsverhältnis, der Erbringung von Sozialleistungen oder diesen gleichgestellten Aufgaben bekanntgeworden sind (Steinbach in Hauck/ Noftz Sozialgesetzbuch, SGB I, Rn. 18 zu § 35 SGB I). Vor diesem Hintergrund war der Argumentation der Staatsanwaltschaft, dass es sich bei den fraglichen Daten nicht um Sozialdaten im Sinne des § 35 SGB I handelt, beizupflichten.

3.14 Darf Personen das Fieber gemessen werden, bevor sie Zugang zu Geschäften oder anderen Einrichtungen bekommen?

Fiebermessen als Voraussetzung dafür, dass eine bestimmte Einrichtung bei einem negativen Ergebnis betreten werden darf, ist in der Regel mangels Eignung und Erforderlichkeit der Messung unzulässig. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden.

Die Corona-Pandemie stellte viele Unternehmen vor Herausforderungen. Ob an Flughäfen, Geschäften oder beim Betreten der Arbeitsstätte versuchten etliche Verantwortliche eine „Sicherheit“ vor der Ansteckungsgefahr zu erreichen, indem sie vor der Gewährung des Zutritts Fieber messen. Nur Personen mit einer normalen Körpertemperatur sollen dann Einlass erhalten. Dies wird damit begründet, dass eine SARS-CoV-2-Infektion teilweise mit einer spezifisch erhöhten Körpertemperatur der infizierten Person einhergeht. So haben sich Arbeitnehmer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt, die sich vor Betreten ihrer Arbeitsstätte erst an der Pforte ein elektronisches Fiebermessgerät an die Stirn halten lassen sollten. Auch Kunden eines Einkaufszentrums wandten sich mit inhaltsgleicher Beschwerde an den TLfDI. Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder unter Beteiligung des Thüringer Landesdaten-

schutzbeauftragten hat sich mit dieser Problematik befasst und ist zu folgendem Ergebnis gekommen:
Für die elektronische Messung der Körpertemperatur zur allgemeinen Regulierung des Zutritts zu Flughäfen, Geschäften, Behörden und Arbeitsstätten können Art. 6 Abs. 1 Satz 1 Buchstabe e), Art. 9 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 3 Bundesdatenschutzgesetz (BDSG) und vergleichbare Vorschriften in den Landesdatenschutzgesetzen (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) beziehungsweise Art. 6 Abs. 1 Satz 1 Buchstabe f), Art. 9 Abs. 2 DS-GVO (Verfolgung eines berechtigten Interesses) als Rechtsgrundlage in Betracht kommen. Auch ist die Messung als betriebliche Maßnahme des Arbeitsschutzes beziehungsweise zur Beurteilung der Arbeitsfähigkeit gestützt auf Art. 88 DS-GVO in Verbindung mit § 26 Abs. 3 BDSG (beziehungsweise das Personaldatenschutzrecht des jeweiligen Landes) oder § 22 Abs. 1 Nr. 1 Buchstabe b) BDSG in Verbindung mit Art. 9 Abs. 2 DS-GVO grundsätzlich denkbar. Nach § 26 Abs. 1 Satz 1 BDSG, ebenso bei § 22 Abs. 1 Nr. 1 Buchstabe b) BDSG und Art. 9 Abs. 2 DS-GVO, muss die Verarbeitung aber auch erforderlich sein. Das heißt, dass eine Verarbeitung von personenbezogenen Daten für den von ihrem verfolgten Zweck geeignet und erforderlich sein muss. Das bedeutet, dass es einen nachweisbaren Einfluss auf das Infektionsgeschehen haben müsste, wenn nur Personen mit einer nicht erhöhten Temperatur zu bestimmten Bereichen Zutritt erhalten.
Genau an dieser Eignung und der Erforderlichkeit der Messung fehlt es aber. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden und viele Infizierte weisen gar keine Symptome und damit auch keine erhöhte Temperatur auf. Diese Patienten sind aber trotzdem ansteckend. Zudem sind mildere Maßnahmen wie zum Beispiel die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der Beschäftigten durch den Arbeitgeber denkbar, die eine nachweisbare Wirkung haben. Damit wäre die Fiebermessung auch nicht verhältnismäßig.
Zur ausführlichen Bewertung wird auf die Veröffentlichung der Datenschutzkonferenz verwiesen: https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waeremebildkameras.pdf.

3.15 Durchführung von Online-Prüfungen an Hochschulen

Sofern eine Rechtsgrundlage besteht, können Prüfungen an Hochschulen auch digital durchgeführt werden. Hinsichtlich der technischen Ausgestaltung eines Online-Prüfungsprogramms muss nach den Anforderungen des Art. 32 DS-GVO sichergestellt werden, dass die Verarbeitung der Daten sicher erfolgt.

Corona und plötzlich machten die Hochschulen dicht. Die Fortführung des Studiums auf digitalem Weg war schon ein Problem, aber wie sollten Prüfungen abgenommen werden, wenn die zu Prüfenden nicht vor Ort sind? Der Thüringer Gesetzgeber wollte hier Abhilfe schaffen. Im Thüringer Gesetz zur Umsetzung erforderlicher Maßnahmen im Zusammenhang mit der Corona-Pandemie (ThürCorPanG) vom 11. Juni 2020 ist in Artikel 14 „Thüringer Gesetz zur Abmilderung der Folgen der Corona-Pandemie im Hochschulbereich“ in § 6 geregelt, dass „die Hochschulen befugt sind, Hochschulprüfungen in elektronischer Form oder in elektronischer Kommunikation (Online-Prüfungen) abzunehmen, sofern die dafür erforderlichen technischen Voraussetzungen und vergleichbare Prüfungsbedingungen gewährleistet sind“. Sie können diese auch außerhalb ihres Standortes durchführen und sich dabei der Hilfe Dritter, auch im Wege der Amtshilfe, bedienen. Hiermit wird eine papierlose Prüfung in elektronischer Form aus der Ferne möglich.
Auch wenn der Datenschutz hier nicht ausdrücklich Erwähnung findet, zu beachten ist er nach der Datenschutz-Grundverordnung (DS-GVO) natürlich stets. Insbesondere bedarf jede Datenübermittlung einer Rechtsgrundlage und die Sicherheit der Verarbeitung muss nach Art. 32 DS-GVO genauso beachtet werden wie der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO. Problematisch gestaltet sich auch die Frage der eindeutigen Identifizierung der zu prüfenden Personen und ein möglicher Rückgriff auf eine Gesichtserkennungssoftware. Dabei handelt es sich um biometrische Daten, die als besondere Kategorien von personenbezogenen Daten nach Art. 9 DS-GVO unter hohen Schutz gestellt sind.
Vor diesem Hintergrund gingen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Nachfragen von Studierenden einer Thüringer Universität ein. Sie hatten Beden-

ken gegen die dort geplante Durchführung von Online-Prüfungen mit einer bestimmten Software.
In rechtlicher Hinsicht kann der Einsatz einer Software zur Durchführung von Online-Prüfungen prinzipiell auf die Ermächtigungsgrundlage des Art. 9 Abs. 2 Buchstabe g) DS-GVO (sofern biometrische Daten verwandt werden), sonst auf Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO) in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) und § 6 Thüringer Gesetz zur Abmilderung der Folgen der Corona-Pandemie im Hochschulbereich gestützt werden. Durch diese Ermächtigungsnorm ist ausschließlich die Verarbeitung zu universitären Zwecken, nämlich zur Durchführung der Online Prüfung, zulässig.
Nach datenschutzrechtlicher Prüfung wurde allen Hochschulen in Thüringen Folgendes mitgeteilt:
Hinsichtlich der technischen Ausgestaltung eines Online-Prüfungsprogramms muss nach den Anforderungen des Art. 32 DS-GVO sichergestellt werden, dass die Übertragung der Daten sicher erfolgt. Es dürfen mithin keinerlei Daten zweckwidrig an Dritte übermittelt werden, schon gar nicht zu Werbe- oder Profilingzwecken.
Es ist unter anderem darauf zu achten, dass das Online-System keine nicht erforderlichen Tracking-Tools verwendet. Beispielsweise hat der von Google-Analytics verwendete Cookie eine andere Qualität als ein „einfacher“ Cookie, da Google die Daten zu beliebigen eigenen Zwecken wie zur Profilbildung nutzt sowie mit anderen Daten verknüpft, siehe hierzu: https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf.
Eine Übermittlung von Daten an Dritte wäre mangels Ermächtigungsgrundlage, wegen Verstoßes gegen den Auftragsverarbeitungsvertrag und auch mangels Erforderlichkeit unzulässig.
Außerdem wies der TLfDI auf Folgendes hin:

- Die Hochschule hat als Verantwortliche die Sicherheit der Datenverarbeitung sicherzustellen.
- Ein Auftragsverarbeitungsvertrag mit der Stelle, bei der die Software bezogen wird, muss abgeschlossen sein.
- Im Auftragsverarbeitungsvertrag muss ausgeschlossen sein, dass Daten für nicht-universitäre Zwecke (eigene Zwecke des Auftragnehmers) verwendet werden. Eine Datenverarbeitung, das heißt, der Einsatz einer Software für Online-Prüfungen darf erst erfolgen, wenn dies garantiert werden kann.

- Falls mit dem Einsatz der Software zur Online-Prüfung biometrische Daten, etwa in Form einer Gesichtserkennung, verarbeitet werden, muss gemäß Art. 35 Abs. 3 Buchstabe b) DS-GVO vorab eine **Datenschutz-Folgenabschätzung** durchgeführt werden. Dies gilt gemäß Art. 35 Abs. 1 DS-GVO auch, wenn die Datenverarbeitung allgemein ein hohes Risiko für Rechte und Freiheiten natürlicher Personen zur Folge hat. Können diese hohen Risiken nicht eingedämmt werden, hat der Verantwortliche *vor* der Datenverarbeitung die Aufsichtsbehörde zu konsultieren.
- Die Hochschule als Verantwortliche ist verpflichtet, eine ordnungsgemäße Information nach Art. 13 DS-GVO vor der Verarbeitung zur Verfügung zu stellen, dies sollte am besten bereits auf der Internetseite der Hochschule erfolgen, spätestens nach dem Log-In.

Der TLfDI machte den Hochschulen ein Gesprächsangebot und empfahl, ihn vor der Einführung entsprechender Systeme rechtzeitig einzubinden.

3.16 Distanzunterricht, was nun? Anforderungen an Videokonferenzsysteme

Vor dem Einsatz eines Videokonferenzsystems muss die datenschutzrechtliche Zulässigkeit von der jeweiligen Schulleitung als Verantwortlicher geprüft werden. Auch der Einsatz von Open-Source-Lösungen wie zum Beispiel BigBlueButton und Jitsi Meet ist zuvor von der Schulleitung zu prüfen.

Da aufgrund der Corona-Pandemie quasi „von jetzt auf gleich“ keine Präsenztreffen mehr wie sonst möglich waren, das tägliche Leben aber weiterging, mussten Alternativen her. In vielen Fällen waren digitale Treffen über Videokonferenzsysteme das Mittel der Wahl. Nicht immer galt bei der Wahl der Systeme der erste Gedanke dem Datenschutz.
Ganz besonders die Schulen waren vor große Herausforderungen gestellt, lebt doch der Schulalltag vom Dialog zwischen Schülern und Lehrern. Auch gab es die Frage, wie während einer Pandemie Leistungsnachweise erbracht werden sollten. Frühzeitig suchte das Thüringer Ministerium für Bildung, Jugend und Sport den Kontakt zum Thüringer Landesbeauftragten für den Datenschutz und die Informa-

tionsfreiheit (TLfDI), um sich von ihm zu den Datenschutzanforderungen an Videokonferenzsysteme beraten zu lassen. Er wies auf Folgendes hin:
Die Frage der Rechtmäßigkeit der Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie der Lehrkräfte durch den Einsatz eines Videokonferenzsystems ergibt sich für die Schule aus Art. 6 Abs. 1 Satz 1 Datenschutz-Grundverordnung (DS-GVO). Danach muss entweder eine Rechtsgrundlage im Schulrecht vorliegen, die die Verarbeitung erlaubt oder hierzu verpflichtet (Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) DS-GVO in Verbindung mit Abs. 2 und 3 in Verbindung mit einer schulrechtlichen Regelung) oder es muss eine Einwilligung der von der Verarbeitung betroffenen Personen vorliegen – bei minderjährigen Schülerinnen und Schülern die Einwilligung der Sorgeberechtigten (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO).
Die Teilnahme an einer Videokonferenz ist *für die Lehrkräfte* allerdings verpflichtend, sofern die Schulleitung dies innerhalb ihrer Organisationsbefugnis festlegt. Hierbei gilt dann Art. 6 Abs. 1 Satz 1 Buchstabe c) in Verbindung mit Abs. 2 und 3 in Verbindung mit Art. 88 DS-GVO in Verbindung mit § 27 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit § 79 Abs. 1 Satz 1 Thüringer Beamtengesetz. In den schulgesetzlichen Bestimmungen von Thüringen sind keine ausdrücklichen Regelungen zum Einsatz von Videokonferenzsystemen enthalten. Die Schulen dürfen gemäß § 57 Abs. 1 Thüringer Schulgesetz nur diejenigen Daten von Schülerinnen und Schülern, Eltern und Lehrkräften verarbeiten, soweit dies für den jeweils mit den Aufgaben verbundenen Zweck erforderlich ist.
Für die Teilnahme an einer Videokonferenz ist eine Einwilligung der Sorgeberechtigten, der volljährigen Schülerin oder des volljährigen Schülers erforderlich. Aus der Verweigerung der Einwilligung dürfen den Schülerinnen und Schülern keine Nachteile erwachsen. In diesen Fällen müssen die Aufgabenstellungen sowie die zugehörigen Arbeitshinweise von den Eltern oder den betreffenden Schülerinnen und Schülern an der Schule abgeholt oder von der Schule postalisch zugesandt werden. Es sollte diesen Schülerinnen und Schülern eine telefonische Erörterung mit einer Lehrkraft angeboten werden.
In der Regel ist die Schule „Verantwortliche“ im Sinne von Art. 4 Nr. 7 DS-GVO. Die Schulleitung vertritt die Schule nach außen und ist unter anderem gegenüber dem Lehrpersonal weisungsberechtigt. Aus diesem Grund darf eine Lehrkraft nicht eigenmächtig ein Video-

konferenzsystem zur Nutzung mit Schülerinnen und Schülern einführen, sondern muss dieses zuvor der Schulleitung zur Genehmigung vorlegen.
Hat die Schulleitung die Nutzung eines bestimmten Videokonferenzsystems ins Auge gefasst, so ist sie als Verantwortlicher verpflichtet, gemäß Art. 24 DS-GVO geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und nachzuweisen, dass die Verarbeitung personenbezogener Daten gemäß der DS-GVO erfolgt. Wird vom Schulträger ein bestimmtes Videokonferenzsystem vorgegeben, so muss dieser grundsätzlich die hinreichenden Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung datenschutzgerecht erfolgt. **Wichtig ist, dass bei Fehlen dieser Voraussetzungen diese nicht im Wege der Einwilligung quasi ersetzt werden können – die Einwilligung ersetzt lediglich die sonst fehlende Rechtsgrundlage, kann aber nicht Verstöße gegen die DS-GVO legalisieren.** Die für die Verarbeitung der Schüler-, Eltern- und Lehrerdaten verantwortliche Schule muss hierüber mit dem Schulträger als Auftragsverarbeiter einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO schließen. Als weitere Möglichkeit können die Schule und der Schulträger gemäß Art. 26 Abs. 1 DS-GVO als gemeinsam für die Verarbeitung Verantwortliche die Zwecke der und die Mittel zur Verarbeitung festlegen. Hierzu müssen die Schule und der Schulträger eine Vereinbarung abschließen, in der insbesondere festgelegt wird, wer von ihnen welche Verpflichtung erfüllt und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DS-GVO nachkommt.
Zur Beantwortung, welche technischen und organisatorischen Maßnahmen getroffen werden müssen, müssen vorab die Kategorien der personenbezogenen Daten bestimmt werden, die während der Videokonferenz zwischen den Schülerinnen und Schülern sowie der Lehrkraft anfallen. Dies sind zum einen die übertragenen Bilder, normalerweise die Gesichter und die getätigten Äußerungen aller Teilnehmenden, zum anderen können dies aber je nach eingesetztem System auch von den Schülerinnen und Schülern erstellte Präsentationen sein. Nicht vorherzusehen, aber mit zu beachten ist das Erfassen von weiteren personenbezogenen Daten, etwa der Hintergrund der Örtlichkeiten (Zimmereinrichtung, Plakate und so weiter) oder auch weiterer Personen, die in den Kamerabereich laufen oder dort sprechen.

Die meisten Videokonferenzsysteme bieten bei der technischen Übertragung eine Transportverschlüsselung an. Dies ist für Unterrichtszwecke im Regelfall auch ausreichend.
Was die Schule in jedem Fall verbieten und im Videokonferenzsystem abschalten muss, ist die Möglichkeit, Videosequenzen mitzuschneiden. In den meisten schulrechtlichen Vorschriften wird die Erstellung von Bild- und Tonaufnahmen mit wenigen Ausnahmen grundsätzlich untersagt.
Die Schule hat grundsätzlich zwei Möglichkeiten, ein Videokonferenzsystem zu betreiben: Entweder wird das System bei einem externen IT-Dienstleister betrieben und die Schule nutzt dieses als Dienstleistung. Dann handelt es sich um einen Online-Dienst, der auch „Software-as-a-Service“ genannt wird. Oder die Videokonferenzsoftware wird auf eigenen Servern oder auf Servern des Schulträgers installiert, dieses Verfahren wird als On-Premise-Betrieb bezeichnet.
Für die Entscheidung für einen Online-Dienst spricht die einfache Nutzung des angebotenen Videokonferenzsystems. Von der Schule muss dann vorab geprüft werden, ob der Anbieter vertrauenswürdig ist und eine ausreichende Datensicherheit nachweisen kann, insbesondere mindestens die Gewährleistung einer Transport-Verschlüsselung. Weiterhin muss von der Schule geprüft werden, wo der Anbieter den Sitz seines Kommunikationsdienstes hat und wo die eingesetzten Server betrieben werden. Hierfür hat die Schule die Datenschutzhinweise und die Geschäftsbedingungen des Anbieters genau durchzuarbeiten. Als Mindestvoraussetzung sollten nur Anbieter ausgewählt werden, die sich im Anwendungsbereich der DS-GVO befinden. Problematisch ist auch, dass Anbieter nur Daten im Auftrag der Schule verarbeiten dürfen, welche vom Verarbeitungszweck schulischen Charakter haben. Verfolgt ein Anbieter auch eigene Zwecke (Analyse von Nutzerverhalten, Datensammlung zu Marketingzwecken, Werbung), so darf die Schule auch hier die Plattform nicht nutzen. Dieser Punkt muss ebenfalls im Vorfeld durch die Schule geklärt werden.
Wenn die Schulen einen Auftragsverarbeitungsvertrag für die Nutzung eines Videokonferenzsystems abschließen müssen (was bei Cloud-Lösungen praktisch immer der Fall ist), haben diese folgendes zu beachten: Die Schule tritt hierbei als Auftraggeber (Verantwortlicher) und der Anbieter als Auftragnehmer (Auftragsverarbeiter) auf. Bei den 2020 angebotenen Systemen hatte die Schule in der Regel keine Möglichkeit, auf den Inhalt des Auftragsverarbeitungsvertrags Einfluss zu nehmen, da es sich in der Regel um ein vom Anbieter vor-

gegebenes Schriftstück handelte. Umso wichtiger ist es für die Schule auch hier, den Vertrag zur Auftragsverarbeitung genau zu lesen und gegebenenfalls Rückfragen zu stellen oder im Zweifel das Vertragswerk nicht zu akzeptieren. Einen Mustervertrag zur Auftragsverarbeitung veröffentlichte der TLfDI unter https://www.tlfdi.de/fileadmin/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf.

Die größten und bekanntesten Anbieter von Videokonferenzprodukten sind allerdings in den USA zu finden. Zum Zeitpunkt des Pandemiegeschehens 2020 war noch rechtlich ungeklärt, ob der CLOUD Act, also ein US-amerikanisches Gesetz, welches unter bestimmten Bedingungen den Zugriff auf gespeicherte Daten durch US-Behörden erlaubt, solange diese nur von amerikanischen IT-Anbietern verarbeitet werden, eine datenschutzgerechte Verarbeitung überhaupt zulässt. Das sogenannte „EU-US Privacy-Shield“, ein Abkommen zwischen der EU und den USA über Zusicherungen zur Einhaltung des in der EU geltenden Datenschutzniveaus, eine der wichtigen Rechtsgrundlagen für den Transfer personenbezogener Daten europäischer Bürger in die USA, wurde vom Europäischen Gerichtshof am 16. Juli 2020 (EuGH C-311/18) für unwirksam erklärt (siehe Beitrag 2.1). Nicht zuletzt aus diesem Grund sehen die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder die Nutzung von Videokonferenzprodukten US-amerikanischer Anbieter äußerst kritisch.

Dem hingegen wird bei der oben genannten „On-Premises“-Lösung das Videokonferenzsystem selbst betrieben. Normalerweise dürften aber der einzelnen Schule hierzu die technischen und personellen Kapazitäten fehlen. Das System kann dann aber zum Beispiel vom Schulträger oder von landeseigenen Stellen gegebenenfalls als landesweiter Einsatz realisiert werden. Dieses ist mit dem Angebot der Thüringer Schulcloud, welche auch ein Videokonferenzsystem enthält, erfolgt, obwohl diese keine On-Premise-Lösung ist, welche auf Thüringer Servern betrieben wird. Dieser Variante sollte aus datenschutzrechtlicher Sicht der Vorzug gegeben werden. Die Videokonferenzlösung der Thüringer Schulcloud entspricht den Anforderungen des Datenschutzes.

Auf der Homepage des TLfDI waren und sind in diesem Zusammenhang auch weitere Hinweise zu Videokonferenzsystemen zu finden. Hierzu zählt unter anderem auch die Auflistung der Berliner Datenschutzbeauftragten (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berli-

ner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf), in der die verschiedenen Systeme bewertet werden und zwischenzeitlich aktualisiert wurden.
In fortgesetzten Schreiben unterrichtete der TLfDI zudem die verantwortlichen Schulleitungen über Videokonferenzsysteme, die er zum damaligen Zeitpunkt empfehlen konnte oder auch nicht.
Schließlich hat der TLfDI in Kooperation mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien 2021 begonnen, in Videokonferenzen den Schulleitungen Rede und Antwort zu Fragen des Datenschutzes im Online-Unterricht zu stehen. Diese Videokonferenzen sind stark nachgefragt und werden bis auf Weiteres fortgesetzt werden.
Im Übrigen wird auf den Beitrag 2.12 zur Orientierungshilfe Videokonferenzsysteme der Konferenz der unabhängigen Datenschutzbeauftragen des Bundes und der Länder verwiesen. Diese Orientierungshilfe und die dazugehörige Checkliste ist unter https://www.tlfdi.de/gesetze/orientierungshilfen/ abrufbar.

3.17 Maskenpflicht in der Schule – Schlagabtausch über Twitter auch in Thüringen

Eine Veröffentlichung von personenbezogenen Daten auf Twitter setzt grundsätzlich die Einwilligung der betroffenen Personen voraus. Etwas anderes gilt für dienstliche Äußerungen von Amtsträgern, die öffentliche Stellen nach außen vertreten. Ein Vorgehen gegen eine unrechtmäßige Veröffentlichung ist nur möglich, wenn der Verantwortliche bekannt ist.

Die Frage, ob und gegebenenfalls ab welchem Alter Schülerinnen und Schüler in der Schule eine Maske tragen müssen, wurde öffentlich heiß diskutiert. Als eine Thüringer Schule einen Schüler nach Hause schickte, weil er außerhalb der Unterrichtsräume keinen Mund-Nasen-Schutz tragen wollte, schrieb der stellvertretende Schulleiter die Eltern an und wies diese auf die an der Schule bestehende Pflicht hin. Dieser Brief fand sich dann nach kurzer Zeit auf Twitter wieder. Das Schreiben enthielt als Adressangaben den Familiennamen und die Wohnanschrift der Eltern und im Text den Namen des Sohnes sowie das ihm vorgeworfene Verhalten und die Aufforderung, die Regeln zum Tragen einer Mund-Nasen-Bedeckung einzuhalten. Darüber hinaus ist vom Unterzeichner des Schreibens der Vor- und Zuname sowie

die Funktion als stellvertretender Schulleiter ersichtlich. In einem Kommentar zu diesem Schreiben war eine Drohung gegenüber dem stellvertretenden Schulleiter und möglicherweise sogar ein Gewaltaufruf zu erkennen.
Zu diesem Vorfall wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) um Stellungnahme gebeten.
So unschön diese Angelegenheit war, hier konnte der TLfDI nur bedingt helfen. Völlig unklar war, wer für den Twittereintrag verantwortlich war und auf welche Weise der Zugriff auf das Schreiben erlangt wurde. Die Identität des Twitterkontoinhabers konnte vom TLfDI nicht ermittelt werden. Damit war ein Vorgehen gegen den Verantwortlichen nicht möglich. Da das eigentliche Problem in der Verknüpfung der Veröffentlichung des Schreibens der Schule mit dem hinzugefügten Kommentar zu liegen schien, wurde insoweit eine Zuständigkeit der Strafverfolgungsbehörden gesehen.
Gleichzeitig konnte auch das Vorliegen eines datenschutzrechtlichen Verstoßes nicht ausgeschlossen werden. Soweit es sich um die personenbezogenen Daten der Adressaten handelt, liegt dann ein datenschutzrechtlicher Verstoß vor, wenn die Betroffenen die Veröffentlichung nicht selbst vorgenommen haben oder nicht ihre Einwilligung in die Veröffentlichung erteilt haben. Waren aber die Adressaten des Schreibens mit der Veröffentlichung einverstanden oder haben diese selbst veranlasst, wäre eine Veröffentlichung dieses Schreibens nicht unbedingt als datenschutzrechtlicher Verstoß der Adressaten zu bewerten.
Weiterhin war zu berücksichtigen, dass es sich um ein amtliches Schreiben der Schule als öffentliche Stelle handelte, welches vom stellvertretenden Schulleiter, der die Schule nach innen und nach außen vertritt, angefertigt und unterzeichnet wurde. Ein schutzwürdiges Interesse des Schulleiters daran, dass ein solches Schreiben von den Adressaten nicht veröffentlicht wird, war deshalb zumindest nicht auf den ersten Eindruck zu erkennen.
Selbstverständlich anders zu bewerten ist die Tatsache, dass das Schreiben in einer Twitternachricht unter Hinzufügung eines Kommentars, aus dem möglicherweise eine Drohung und ein Gewaltaufruf entnommen werden können, verwendet wird. Dieser Sachverhalt war in erster Linie strafrechtlich zu verfolgen, aber kein datenschutzrechtliches Problem. Dies wurde dem stellvertretenden Schulleiter mitgeteilt. Es wurde ihm geraten, sich in diesem Zusammenhang mit der

Polizei in Verbindung zu setzen. Außerdem wurde er darauf aufmerksam gemacht, dass er unter dem Link https://help.twitter.com/de/rules-and-policies/violent-threats-glorification eine Löschung des Twittereintrags beantragen könne, wenn eine Gewaltandrohung im Tweet enthalten ist.
Der betreffende Eintrag findet sich mittlerweile nicht mehr auf Twitter, weil das Konto gesperrt wurde.

3.18 Umsetzen des Masernschutzgesetzes in der Schule

Die Erhebung von Impfdaten ist aufgrund des Masernschutzgesetzes datenschutzrechtlich zulässig. Allerdings müssen die Vorgaben des Gesetzes eingehalten werden. Eine Kopie und ihre Speicherung der personenbezogenen Daten sind nicht erforderlich.

Das Masernschutzgesetz gilt seit dem 1. März 2020. Danach müssen alle nach 1970 geborenen Personen, die in einer Gemeinschaftseinrichtung betreut werden, den Impfschutz gegen Masern nachweisen. Das Gesetz dient dem Zweck, den Impfschutz dort zu erhöhen, wo eine Masern-Übertragung sehr schnell stattfinden kann, wenn nicht genügend Personen gegen Masern immun sind, und dort vor allem die Personen schützen, die nicht selbst gegen Masern geimpft werden können, zum Beispiel, weil sie schwanger sind oder ein sehr schwaches Immunsystem haben.
Aus datenschutzrechtlicher Sicht stellt das Gesetz eine Rechtsgrundlage für die Erhebung des Datums dar, ob eine Person bereits gegen Masern geimpft ist oder nicht. Bei der Organisation des Nachweises ist aber zu beachten, dass die Tatsache des Impfstatus das Tatbestandsmerkmal der besonderen Kategorien von personenbezogen Daten erfüllt, weil es ein Gesundheitsdatum ist. Diese Daten sind nach der Datenschutz-Grundverordnung (DS-GVO) unter besonderen Schutz gestellt.
Etliche Bürger in Thüringen waren besorgt, ob die Einrichtung, die den Nachweis der Masernimpfung prüfen muss, also die Schule oder Kindertagesstätte, die einzuhaltenden Datenschutzbestimmungen beachteten.
In einem Fall enthielt die Elterninformation der Leitung einer Schule die Festlegung, dass die Klassenlehrerin die Prüfung des Nachweises übernimmt. Ein besorgter Elternteil erkundigte sich, ob allein auf der

Grundlage des Infektionsschutzgesetzes Schulleiter beziehungsweise Klassenleiter mit dieser Aufgabe betraut werden dürfen.
Die einschlägige Bestimmung des § 20 Abs. 9 Infektionsschutzgesetz führt dazu Folgendes aus:
„Personen, die in Gemeinschaftseinrichtungen nach § 33 Nummer 1 bis 3 […] betreut werden sollen, haben der Leitung der jeweiligen Einrichtung vor Beginn ihrer Betreuung oder ihrer Tätigkeit folgenden Nachweis vorzulegen:
1. eine Impfdokumentation nach § 22 Abs. 1 und 2 oder ein ärztliches Zeugnis, auch in Form einer Dokumentation nach § 26 Abs. 2 Satz 4 des Fünften Buches Sozialgesetzbuch, darüber, dass bei ihnen ein nach den Maßgaben von Absatz 8 Satz 2 ausreichender Impfschutz gegen Masern besteht,
2. ein ärztliches Zeugnis darüber, dass bei ihnen eine Immunität gegen Masern vorliegt oder sie aufgrund einer medizinischen Kontraindikation nicht geimpft werden können **oder**
3. eine Bestätigung einer staatlichen Stelle oder der Leitung einer anderen in Absatz 8 Satz 1 genannten Einrichtung darüber, dass ein Nachweis nach Nummer 1 oder Nummer 2 bereits vorgelegen hat.
[…] Wenn der Nachweis nach Satz 1 von einer Person, […] nicht vorgelegt wird oder wenn sich ergibt, dass ein Impfschutz gegen Masern erst zu einem späteren Zeitpunkt möglich ist oder vervollständigt werden kann, hat
1. die Leitung der jeweiligen Einrichtung oder
2. die andere Stelle nach Satz 2 oder Satz 3
unverzüglich das Gesundheitsamt, in dessen Bezirk sich die Einrichtung befindet, darüber zu benachrichtigen und dem Gesundheitsamt personenbezogene Angaben zu übermitteln.“
Nach dem Gesetzestext hat also der Leiter der Einrichtung die entsprechenden Impfdokumente zu prüfen. Da die Schulleitung aber gegenüber den Lehrkräften weisungsberechtigt ist, kann sie die Kontrolle des Nachweises für eine effektivere Umsetzung auch delegieren.
Die Datenerhebung an sich ist wegen der gesetzlichen Verpflichtung nach Art. 6 Abs. 1 Satz 1 Buchstabe e) in Verbindung mit Abs. 3 Buchstabe b) DS-GVO und § 29 Abs. 9 des Infektionsschutzgesetzes zulässig. Selbstverständlich müssen dabei alle anderen Anforderungen der DS-GVO eingehalten werden.
Dabei ist es wichtig, sich an die Vorgabe der Rechtsgrundlage zu halten. Der Nachweis kann auf die drei in der Vorschrift genannten Weisen erbracht werden, das wird durch die Verwendung des Wortes

„oder“ deutlich. Eine Gemeinschaftseinrichtung kann daher nicht einfach eine bestimmte Form des Nachweises verlangen.
Die Datenerhebung muss sich auch am Grundsatz der Erforderlichkeit orientieren. Nach § 16 Abs. 1 Satz 1 des Thüringer Datenschutzgesetzes ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Gleiches gilt für nicht-öffentliche Stellen nach Art. 5 Abs. 1 Buchstabe c) DS-GVO. Für den Nachweis der Masernimpfung reicht es aus, wenn der Impfausweis der betroffenen Person oder das ärztliche Zeugnis der Einrichtung vorgelegt wird. Eine Kopie und ihre Speicherung sind nicht erforderlich. Dementsprechend wurden durch das Thüringer Ministerium für Bildung, Jugend und Sport entsprechende Formulare für den Nachweis des Impfschutzes bei Schülern und Beschäftigten entwickelt.
Weitere hilfreiche Informationen rund um das Thema Masernschutzgesetz finden Sie unter https://bildung.thueringen.de/schule/aktiv/gesundheit.

3.19 Vorlage des Steuerbescheides im Beihilfeverfahren

Im Berichtsjahr erreichten den TLfDI Anfragen beihilfeberechtigter Personen, die zum Nachweis des Einkommens ihrer berücksichtigungsfähigen Angehörigen gemäß § 3 Abs. 1 Satz 2 Nr. 1 ThürBhV den vollständigen Steuerbescheid des vorangegangenen Jahres gegenüber dem Thüringer Landesamt für Finanzen vorlegen sollten. Um das Einkommen des Angehörigen nachprüfen zu können, darf sich die Beihilfestelle grundsätzlich den vollständigen Einkommensteuerbescheid der Eheleute/ Lebenspartner vorlegen lassen – jedenfalls soweit hieraus die Beträge für den Angehörigen hervorgehen, der kostenfrei mitversichert werden soll. Datenschutzrechtliche Belange stehen dem nicht entgegen.

Beihilfeberechtigte Personen (§ 2 Abs. 1 und 2 Thüringer Beihilfeverordnung – ThürBhV), deren Angehörige (Ehegattin/ Ehegatte, eingetragene Lebenspartnerin/ eingetragener Lebenspartner) mitversichert sind oder werden sollen, wandten sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und fragten an, ob die von der Beihilfestelle zur Prüfung der Einkommensgrenze gemäß § 3 Abs. 1 Satz 2 Nr. 1 ThürBhV verlangte Vorlage des

vollständigen Einkommensteuerbescheides der Eheleute/ eingetragenen Lebenspartner rechtens sei. Das Problem ist nicht neu. Der TLfDI kannte dieses Problem bereits vor Geltung der Datenschutz-Grundverordnung (DS-GVO). Die Lösung ist vor wie nach In-Kraft-Treten der DS-GVO gleich: Ja, die Beihilfestelle darf die Vorlage des vollständigen Steuerbescheides verlangen, soweit hieraus das Einkommen der/ des Angehörigen hervorgeht, den es zu überprüfen gilt. Maßgeblich hierfür ist der Grundsatz der Erforderlichkeit gemäß § 16 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Danach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Vorliegend ist die Beihilfestelle verpflichtet zu prüfen, ob eine/ ein Angehöriger einer beihilfeberechtigten Person unter die Vorschrift des § 3 Abs. 1 Satz 2 Nr. 1 ThürBhV fällt, mithin kostenfrei mitzuversichern ist. Dabei darf der Gesamtbetrag der Einkünfte (§ 2 Abs. 3 und 5a Einkommensteuergesetz – EStG) des Angehörigen im zweiten Kalenderjahr vor der Stellung des Beihilfeantrages 18.000 Euro nicht übersteigen. Anknüpfungspunkt ist der Gesamtbetrag der Einkünfte gemäß § 2 Abs. 3 EStG. Damit fließen alle Einkünfte des Angehörigen gemäß § 2 Abs. 1 Nr. 1 bis 7 EStG in die Berechnung der Höchstgrenze nach § 3 Abs. 1 Satz 2 Nr. 1 ThürBhV mit ein. Der ausgewiesene Gesamtbetrag der Einkünfte ist gemäß § 2 Abs. 5a EStG gegebenenfalls zu erhöhen oder zu mindern. Die dafür maßgeblichen Angaben können jedoch nur einem vollständigen Steuerbescheid entnommen werden. Nur anhand des Steuerbescheids kann die Beihilfestelle auch nachvollziehen, ob die Angaben aus dem für die Beihilfegewährung relevanten Jahr stammen. Demzufolge besteht für die Beihilfestelle eine Erforderlichkeit zur Datenverarbeitung gemäß § 16 Abs. 1 ThürDSG.

Betreffen die Angaben im Steuerbescheid ausschließlich die beihilfeberechtigte Person selbst, so sind diese indes nicht zur Prüfung der Mitversicherung gemäß § 3 Abs. 1 Satz 2 Nr. 1 ThürBhV erforderlich und dürfen folglich vom Antragsteller unkenntlich gemacht werden. Dies gebietet der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Allerdings dürfen Überlegungen des Antragstellers, dass einzelne Angaben auch bezüglich des Angehörigen mög-

licherweise nicht erforderlich seien, nicht zu einer Beschränkung der Prüfungsmöglichkeit durch die Beihilfestelle führen.
Weitere Informationen zu den erforderlichen Angaben enthält das Formblatt „Erklärung zu den Einkünften der Ehegattin/ des Ehegatten, der Lebenspartnerin/ des Lebenspartners des Thüringer Landesamtes für Finanzen, Beihilfestelle“, abrufbar unter: https://thformular.thueringen.de/thueform/cfs/eject/pdf/2502.pdf?MANDANTID=18&FORMUID=THUERBHV-008-TH-FL.

3.20 Umgang mit Personalakten zur Vorbereitung der Neugliederung kreisangehöriger Gemeinden

Werden Gemeinden oder Landkreise neu gegliedert, so ergeben sich zwangsläufig auch datenschutzrechtliche Probleme. Was passiert mit den bestehenden Arbeitsverhältnissen? Darf sich eine neu gegründete Gemeinde von der vormals zugehörigen Verwaltungsgemeinschaft im Rahmen der Neugliederungsmaßnahmen detaillierte Daten der Beschäftigten der Verwaltungsgemeinschaft (vollständige Namen aller Beschäftigten, arbeitsvertraglich vereinbarte Entgeltgruppen, Beschäftigungsgruppen, Eintritt in die Altersrente) vorlegen lassen, um die „Übernahme“ von Personal zu planen? Die Antwort: Nicht ohne Einwilligung der betroffenen Beschäftigten.

Eine Verwaltungsgemeinschaft aus Nordthüringen wandte sich im Dezember 2019 an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da sie Bedenken hinsichtlich der Herausgabe von Beschäftigtendaten der bei ihr Beschäftigten an eine noch neu zu bildende Stadt beziehungsweise Landgemeinde aus ihrer Verwaltungsgemeinschaft hatte. Hintergrund war die geplante Ausgliederung von zwei Kommunen aus der Verwaltungsgemeinschaft zum 1. Januar 2021 gemäß § 6 Abs. 1 des Zweiten Thüringer Gesetzes zur freiwilligen Neugliederung kreisangehöriger Gemeinden im Jahr 2019 (2. ThürGNGG 2019). Gleichzeitig sollte aus den beiden aufgelösten Kommunen und einer ebenfalls aufgelösten Gemeinde die neue Landgemeinde gebildet werden (§ 6 Abs. 2 Satz 2 des 2. ThürGNGG 2019). Details der Neugliederung der betroffenen Kommunen sollten im Rahmen einer Auseinandersetzung festgelegt werden (§ 6 Abs. 6 des 2. ThürGNGG 2019). Der Bürgermeister der bis zum 31. Dezember 2020 bestehenden Stadt erbat von der Verwaltungsgemeinschaft eine Übersicht mit umfangreichen Personaldaten

(Name, Vorname, arbeitsvertraglich vereinbarte Entgeltgruppe, frühestmöglicher Eintritt in die Altersrente) der Beschäftigten der Verwaltungsgemeinschaft, um die bevorstehende Auseinandersetzung personell zu planen. Hierzu sollte eine nicht näher beschriebene Arbeitsgruppe für die geplante Ausgliederung eingesetzt werden, die Einblick in diese sensiblen Beschäftigtendaten der Beschäftigten der Verwaltungsgemeinschaft erhalten sollte. Der Gemeinschaftsvorsitzende der Verwaltungsgemeinschaft hatte berechtigte Zweifel an der datenschutzrechtlichen Zulässigkeit einer solchen Herausgabe von Daten und bat den TLfDI um eine rechtliche Einschätzung.
Der TLfDI bestätigte diese Zweifel aus nachfolgenden Gründen:
Zweifellos sind Vorbereitungshandlungen, die regelmäßig auch den künftigen Personaleinsatz betreffen, im Rahmen solcher Neugliederungsmaßnahmen notwendig. Es bedarf allerdings einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Beschäftigten.
Zunächst handelt es sich bei den erbetenen Daten zweifelsfrei um personenbezogene Daten von Beschäftigten der Verwaltungsgemeinschaft. Diese sind der Verwaltungsgemeinschaft als personalverwaltenden und beschäftigenden Stelle zugeordnet. Damit ist die öffentliche Stelle, hier die Verwaltungsgemeinschaft, die die Daten vorlegen soll, für die Zulässigkeit einer solchen Herausgabe der Daten der bei ihr Beschäftigten datenschutzrechtliche Verantwortliche (Art. 4 Nr. 7 Datenschutz-Grundverordnung). § 27 Abs. 1 Thüringer Datenschutzgesetz bestimmt in Verbindung mit § 85 Abs. 1 Thüringer Beamtengesetz (ThürBG), unter welchen Voraussetzungen Personalaktendaten, zu denen diese Daten gehören, und Auskünfte an Dritte erteilt werden dürfen. Dabei wird man bei einer Neugliederung von Kommunen oder wie hier, dem Austritt einer Kommune aus der Verwaltungsgemeinschaft, die austretende Stadt beziehungsweise die neu zu bildende Gemeinde als Dritte ansehen müssen. Vorliegend lagen zum Zeitpunkt der Anfrage beim TLfDI die Voraussetzungen für eine solche Datenübermittlung gemäß § 85 Abs. 1 Satz 2 ThürBG noch nicht vor, da das Vorbereitungsstadium noch nicht in ein konkretes Auswahlverfahren übergegangen war. Insoweit darf der Zugang zu Personalaktendaten nur befugten Personen gestattet werden (§ 80 ThürBG).
Zwar beinhaltet das 2. ThürGNGG 2019 in § 23 eine Regelung zur Rechtsstellung der betroffenen Tarifbeschäftigten der von der Neugliederung betroffenen Gemeinden, die besagt, dass – parallel zum Betriebsübergang gemäß § 613a Bürgerliches Gesetzbuch – eine

„Übernahme“ des Personals in die neu gebildete oder erweiterte Verwaltungsgemeinschaft erfolgt. Diese Regelung betraf vom Wortlaut her jedoch das Personal der weiter bestehenden, wenn auch verkleinerten, Verwaltungsgemeinschaft, nicht das „neue“ Personal der neu gegründeten Stadt beziehungsweise Landgemeinde.
Der TLfDI sah es im konkreten Fall lediglich als zulässig an, in Vorbereitung des künftigen Personalbedarfs der Landgemeinde eine Liste der derzeitigen Stellenbesetzung in der Verwaltungsgemeinschaft, wie sie auch der kommunale Haushaltsplan enthält, zu erstellen oder den Stellenplan der Verwaltungsgemeinschaft heranzuziehen. Dabei sollte auf eine Anonymisierung geachtet werden, die einen Rückschluss auf einzelne Beschäftigte ausschließt. Konkrete Daten der Beschäftigten der bisherigen Verwaltungsgemeinschaft jedenfalls hätten zum Zeitpunkt der Anfrage nur mit ausdrücklicher und schriftlicher Einwilligung der Beschäftigten herausgegeben werden dürfen, wobei besonderes Augenmerk auf die Freiwilligkeit einer solchen Einwilligung zu legen wäre (vgl. Gesetzentwurf der Landesregierung zum Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz EU – ThürDSAnpUG-EU), Drucksache 6/4943 des Thüringer Landtags, hier Begründung zu § 27 Abs. 2, Seiten 113 und 114, abrufbar unter: http://www.parldok.thueringen.de/ParlDok/dokument/65346/thueringer_gesetz_zur_anpassung_des_allgemeinen_datenschutzrechts_an_die_verordnung_eu_2016_679_und_zur_umsetzung_der_richtlinie_eu_2016_680_thueringe.pdf).
Jeglicher Druck auf die Beschäftigten lässt die Freiwilligkeit entfallen mit der Folge, dass die Einwilligung als unwirksam anzusehen wäre.
Hinsichtlich der weiteren Auseinandersetzungsverhandlungen der Kommunen sollte aus Sicht des TLfDI weiter darauf geachtet werden, dass nur festgelegte Personen mit ausdrücklicher Personalverantwortung und entsprechenden besonderen Verschwiegenheitsverpflichtungen mit Personalentscheidungen betraut werden.

3.21 Veröffentlichung von Beschäftigtendaten auf der Internetseite

Firmen-Webseiten, Facebook, Instagram, Twitter – auch wenn Internetdienste und soziale Netzwerke mittlerweile für viele Betriebe und private Organisationen ein probates und beliebtes Mittel der Öffent-

lichkeitsarbeit darstellen, ist bei der Ausgestaltung dieser Onlinedienste Vorsicht geboten. Dies nicht nur, weil die Betreiber solcher Dienste im Hintergrund Daten sammeln. Besonders bei der Veröffentlichung von Beschäftigtendaten sollte die verantwortliche Stelle vorher hinterfragen, ob eine Veröffentlichung solcher Daten überhaupt zulässig ist. Gesteigerte Zulässigkeitsvoraussetzungen gelten zudem bei besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO, zum Beispiel Gesundheitsdaten. Eine Veröffentlichung solch sensibler Daten ist – von wenigen denkbaren Ausnahmen abgesehen – unzulässig.

Internet und soziale Medien – oder auch „die digitale Welt“ – gehören heute zum Alltag vieler Menschen dazu. Auch Betriebe nutzen Internetdienste, um über ihr Leistungsangebot, aktuelles Firmengeschehen oder ihre Firmengeschichte zu informieren. Oftmals werden dabei auch Beschäftigtendaten (Name, Funktion, Lebenslauf, Fotos et cetera) veröffentlicht. Nur selten fragen sich die Verantwortlichen dabei, wie es hierbei um den Datenschutz bestellt ist. Grundsätzlich ermöglicht das Grundrecht auf informationelle Selbstbestimmung jeder Person, selbst darüber entscheiden zu dürfen, welche Daten sie von sich preisgibt. Schnell können Informationen auch zum Nachteil der Beschäftigten verwendet werden, etwa durch Profilbildung.
In dem Fall einer Beschwerde einer Mitarbeiterin einer politischen Partei aus Thüringen hat die verantwortliche Partei – wie sich später herausstellte unbeabsichtigt – einen Protokollentwurf einer Telefonkonferenz ihres Landesvorstandes auf der Webseite veröffentlicht. In der Sitzung ging es unter anderem um Personalfragen, über die der Landesvorstand zu befinden hatte. Betroffen hiervon war auch die Beschwerdeführerin. Dabei kam es zur Nennung des, wenn auch zum Teil abgekürzten, Namens der Beschwerdeführerin sowie Details ihres Gesundheitszustandes.
Die Beschwerdeführerin beschwerte sich zu Recht beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser leitete eine Anhörung gegenüber der verantwortlichen Partei ein. Daraufhin bemerkte die Verantwortliche den Fehler und entfernte den versehentlich veröffentlichten Protokollentwurf von ihrer Webseite. Häufig sind gelöschte Inhalte auch nach einem Entfernen von der Webseite noch im Cache von Google vorzufinden, sodass dem Löschungsanspruch gemäß Art. 17 Datenschutz-Grundverordnung (DS-GVO) noch nicht Genüge getan ist. Dabei verpflichtet

Art. 17 Abs. 2 DS-GVO Verantwortliche, „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art“ in die Wege zu leiten, um auch andere Verantwortliche, die Daten der löschungsbegehrenden Person verarbeiten, von dem Löschungsanspruch zu informieren, damit im Ergebnis sämtliche Links zu den personenbezogenen Daten oder zu Kopien oder Replikationen gelöscht werden. In der Praxis bedeutet dies auch die Löschung von entsprechenden Links aus den gängigen Suchmaschinen wie Google. Der Internetdienst stellt Informationen zum Entfernen von Daten in seiner Suchmaschine und einen Antrag auf Entfernen zur Verfügung unter: https://support.google.com/websearch/troubleshooter/3111061. Auch dem kam die Verantwortliche im Beschwerdefall nach.

3.22 Was darf an personenbezogenen Daten außerhalb des behördlichen Arbeitsplatzes verarbeitet werden? Telearbeit und neue Formen des Arbeitens unter Corona

Auch die Thüringer Landesverwaltung wurde im Zuge der Corona-Pandemie vor Herausforderungen bei der Gewährung von Telearbeit oder Möglichkeiten der mobilen Arbeitsgestaltung gestellt. Verträgt sich das Arbeiten im häuslichen Umfeld oder gar mobil an flexiblen Orten überhaupt mit dem Datenschutz und wenn ja, welche Anforderungen müssen hierbei beachtet werden? Datenschutzrechtlich nicht immer einfach – aber nicht unmöglich. Der Beitrag gibt erste Hinweise, wie Telearbeit und mobiles Arbeiten auch in der öffentlichen Verwaltung gelingen können.

Das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung einer Dienstvereinbarung, die es den Tarifbeschäftigten, Beamten, Staatsanwälten und Richtern der Thüringer Gerichte und Staatsanwaltschaften künftig ermöglichen soll, einen Teil ihrer dienstlichen Tätigkeit von „mobilen Arbeitsplätzen aus“ zu verrichten. Folgende Empfehlungen und Hinweise sprach der TLfDI gegenüber dem Ministerium aus:

- Zwischen Telearbeit und mobilem Arbeiten muss unterschieden werden. Telearbeit ist in der Regel an den häuslichen Bereich gebunden. Der häusliche Arbeitsplatz kann dabei durch elektronische Informationsverarbeitungs- und Kommunikationsmittel mit

der Dienststelle verbunden sein. Mobiles Arbeiten ermöglicht im Unterschied zur Telearbeit ortsunabhängiges Arbeiten. Auch hierbei kann in der Regel mittels mobiler Informations- und Kommunikationstechnik auf die behördeninterne IT-Infrastruktur zugegriffen werden.

- Eine klare gesetzliche Regelung für Telearbeit/ mobiles Arbeiten gibt es nicht. Datenschutzrechtliche Bestimmungen schließen beide Tätigkeiten jedoch nicht aus. Der Dienstherr muss festlegen, welche Voraussetzungen im Einzelfall vorliegen müssen, damit die jeweilige Arbeitsform vertretbar ist. Dabei sind immer die Gefahren für die Persönlichkeitsrechte der Personen, deren Daten verarbeitet werden und mithin betroffen sind, maßgeblich. Einfach ausgedrückt gilt: Je höher die Sensibilität der Daten ist, desto höher ist auch ihr Schutzbedarf und folglich sind es auch die zu ergreifenden Schutzmaßnahmen in technischer und organisatorischer Hinsicht.
- Bei einer Genehmigung von Telearbeit/ mobilem Arbeiten durch den Dienstherrn ist stets zu berücksichtigen, dass dieser in der Regel nur eingeschränkte Kontroll- und Einflussmöglichkeiten auf die Einhaltung datenschutzrechtlicher Belange im häuslichen Bereich der Beschäftigten hat. Da der Dienstherr jedoch auch bei einer genehmigten Telearbeit/ mobilem Arbeiten grundsätzlich die datenschutzrechtliche Verantwortung für die personenbezogenen Daten trägt, sollten die Datenschutzgrundsätze für Telearbeit/ mobiles Arbeiten, insbesondere die vom Dienstherr und Beschäftigten zu beachtenden Schutzmaßnahmen sowie Kontrollrechte und -pflichten in einer Dienstvereinbarung festgeschrieben werden.
- Besondere Vorsicht ist dabei geboten, wenn besonders schützenswerte Daten, zum Beispiel Gesundheits-, Beschäftigten- oder Sozialdaten, in Telearbeit/ mobilem Arbeiten verarbeitet werden sollen. Datenschutzrechtliche Bestimmungen beinhalten nicht per se ein Verbot der Verarbeitung solcher Daten auch im häuslichen Bereich oder mobil. Jedoch obliegt es dem verantwortlichen Dienstherrn, die entsprechend dem Schutzniveau der Daten erforderlichen Schutzvorkehrungen im Einzelfall zu treffen. Dies kann auch dazu führen, dass der Dienstherr die Verarbeitung solch höchst sensibler Daten in Telearbeit/ mobilem Arbeiten untersagt. Lassen sich im Einzelfall nicht die erforderlichen technischen (zum Beispiel Zwei-Faktor-Authentifizierung, gesicherter VPN-

Zugang, Verschlüsselungstechniken, Anbindung an Remote-Desktop Lösungen) und organisatorischen Maßnahmen (zum Beispiel Vorhandensein eines separaten Arbeitszimmers im häuslichen Bereich, verschließbare Aufbewahrungsmöglichkeit der Zugangsmittel und lokal gespeicherten Daten) herstellen, so bedeutet dies das „Aus“ einer Verarbeitung solcher Daten außerhalb der Dienststelle. Die Entscheidung darüber, ob und welche Daten auch außerhalb der Dienststelle wie verarbeitet werden dürfen, trifft letztlich der Dienstherr.

Weitergehende Informationen rund um das Thema „Telearbeit und Mobiles Arbeiten“ finden sich im gleichlautenden Datenschutz-Wegweiser des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, herausgegeben im Juli 2020, veröffentlicht unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.pdf;jsessionid=D1410A1B78C5A39C7632E9BD1CBDD46E.2_cid329?__blob=publicationFile&v=32.

Weitere Hinweise zu dem Thema finden sich beim Bundesamt für Sicherheit in der Informationstechnik, im „IT-Grundschutz-Kompendium“ (Stand 2021), hier ab Seite 231 „OPS.1.2.4: Telearbeit“ und ab Seite 775 „INF.8: Häuslicher Arbeitsplatz“, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

3.23 Vorgänge, die innerhalb der Bundesrepublik vom TLfDI an andere LfD’s abgegeben wurden

Der TLfDI kontrolliert gemäß § 37 ThürDSG bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 34 ThürDSG in Verbindung mit § 38 Abs. 6 BDSG Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Die örtliche Zuständigkeit richtet sich grundsätzlich nach dem Sitz der für die Datenverarbeitung verantwortlichen Stellen beziehungsweise nach dem Ort einer Betriebsstätte. Der TLfDI ist oft, aber nicht immer zuständig!

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum über 200 Anfragen und Beschwerden von besorgten Bürgern, die nicht in seinen

Zuständigkeitsbereich fielen. Da wären zum Beispiel Beschwerden aus dem Bereich der Telekommunikation (Telefonanbieter). Für die Datenschutzkontrolle in diesem Bereich ist in jedem Fall der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) mit Sitz in 53117 Bonn, Husarenstraße 30, (E-Mail: poststelle@bfdi.bund.de) zuständig. Diese Zuständigkeit ist unabhängig davon gegeben, wo das Unternehmen seinen Hauptsitz in Deutschland hat (§ 115 Abs. 4 Telekommunikationsgesetz).
Sofern ein Unternehmen seine Niederlassung in Deutschland hat, ist die Aufsichtsbehörde in dem betreffenden Bundesland zuständig. So besteht beispielsweise bei Beschwerden und Anfragen über die Firma Google und ihren weiteren Firmen wie YouTube für die Kontrolle der Verarbeitung personenbezogener Daten die Zuständigkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Ludwig-Erhard-Straße 22 in 20459 Hamburg.
Der Bereich des Rundfunks ist aus verfassungsrechtlichen Gründen aus der Kontrollbefugnis der Landesbeauftragten ausgenommen. Wegen der Unabhängigkeit und der Staatsferne des öffentlich-rechtlichen Rundfunks gibt es Besonderheiten der Datenschutzkontrolle. Die datenschutzrechtliche Aufsicht über die Verarbeitung personenbezogener Beitragsschuldnerdaten beim Beitragsservice von ARD, ZDF und Deutschlandradio obliegt nicht den Landesbeauftragten für den Datenschutz. Die datenschutzrechtliche Kontrollkompetenz besteht grundsätzlich bei den jeweils zuständigen Rundfunkdatenschutzbeauftragten der betroffenen Rundfunkanstalt. Im Falle des Mitteldeutschen Rundfunks (MDR) ist es der Datenschutzbeauftragte des Mitteldeutschen Rundfunks, Kantstraße 71 – 73 in 04275 Leipzig.
Des Weiteren gingen im Berichtszeitraum viele Anfragen zu und Beschwerden über unterschiedliche Thüringer Jobcenter ein. Die Jobcenter gehören zum größten Teil zur Bundesagentur für Arbeit. Diese fallen in den datenschutzrechtlichen Zuständigkeitsbereich des BfDI. Es besteht aber auch die Möglichkeit, dass die Kommunen Jobcenter in eigener Zuständigkeit betreiben. Das sind die so genannten „Optionskommunen“. Der TLfDI ist für die Jobcenter nur zuständig, sofern es sich um diese Optionskommunen in Thüringen handelt. Diese sind das Jobcenter Jena, der Landkreis Eichsfeld, der Landkreis Greiz und der Landkreis Schmalkalden-Meiningen.
Für die Kontrolle der Verarbeitung personenbezogener Daten durch kirchliche Stellen sind aufgrund des besonderen Status von Religionsgemeinschaften die Regelungen über die Datenschutzaufsicht der DS-

GVO grundsätzlich nicht anwendbar. Die Evangelischen Kirchen und die Bistümer der Katholischen Kirche haben eigene Datenschutzvorschriften erlassen, die aber mit den Regelungen der DS-GVO in Einklang stehen müssen. Deshalb haben die Evangelischen Kirchen und die Katholischen Bistümer auch eigene Datenschutzbeauftragte. Für die Evangelische Kirche in Thüringen ist der Beauftragte für den Datenschutz der EKD, Außenstelle Berlin, Invalidenstraße 29 in 10115 Berlin zuständig.
Für die katholischen Kirchen in Thüringen ist der Datenschutzbeauftragte des Bistums Erfurt, Bischöfliches Ordinariat, Herrmannsplatz 9 in 99084 Erfurt für Datenschutzverstöße zuständig.
Auch wenn es um datenschutzrechtliche Fragen und Beschwerden zu parlamentarischen Angelegenheiten des Thüringer Landtags geht, ist der TLfDI **nicht** die zuständige Aufsichtsbehörde. Dies ergibt sich bereits aus § 2 Abs. 6 Satz 3 und Satz 4 Thüringer Datenschutzgesetz (ThürDSG). Zuständig ist vielmehr gemäß § 1 Abs. 1 in Verbindung mit § 17 Abs. 1 Satz 1 der Parlamentarischen Datenschutzordnung der Ältestenrat des Thüringer Landtags.
Für den Thüringer Rechnungshof ist der TLfDI gemäß § 2 Abs. 9 Satz 1 ThürDSG nur als Aufsichtsbehörde zuständig, soweit ersterer in Verwaltungsangelegenheiten tätig wird. Damit wird die unabhängige Stellung des Rechnungshofs zwecks Überwachung der gesamten Haushalts- und Wirtschaftsführung des Freistaats Thüringen hinreichend berücksichtigt.
Gleiches gilt für die Thüringer Justiz: Für sie ist der TLfDI nur insoweit als datenschutzrechtliche Aufsichtsbehörde zuständig, als dass die Gerichte in Verwaltungsangelegenheiten tätig werden. Das bedeutet im Umkehrschluss: Für jegliche datenschutzrechtlichen Fragen, die die richterliche Unabhängigkeit betreffen (zum Beispiel die Ladung oder Vernehmung von Zeugen oder die Beweiswürdigung einschließlich der Urteilsverkündung) ist nicht der TLfDI, sondern der/ die Datenschutzbeauftragte des jeweiligen Gerichts der richtige Ansprechpartner/ die richtige Ansprechpartnerin.

3.24 Öffentlich bestellte Vermessungsingenieure (Sammelbeitrag)

Nach Art. 6 DS-GVO muss eine Verarbeitung personenbezogener Daten rechtmäßig sein. Wie der folgende Sachverhalt darstellt, kann § 18 des Thüringer Vermessungs- und Geoinformationsgesetzes eine Er-

laubnisnorm nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO zur Datenverarbeitung darstellen. Öffentlich bestellte Vermessungsingenieure sind öffentliche Stellen im Sinne von § 2 ThürDSG. Sie haben gemäß Art. 37 Abs. 1 DS-GVO in Verbindung mit § 13 Abs. 1 ThürDSG einen Datenschutzbeauftragten zu bestellen.

An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte sich ein besorgter Immobilienbesitzer, der sich in seinem Grundrecht auf informationelle Selbstbestimmung verletzt fühlte. Er teilte dem TLfDI mit, dass er ein Schreiben einer Immobilienfirma erhalten habe, in dem die Immobilienfirma zum wiederholten Male Kaufinteresse an seiner Immobilie in Erfurt erklärt hatte. Da dem Immobilienbesitzer das Immobilienunternehmen gänzlich unbekannt war, bat er zunächst das Immobilienunternehmen um Auskunft, woher es Kenntnis davon hatte, dass er Eigentümer einer Immobilie in Erfurt sei. Daraufhin erhielt er von dem Immobilienunternehmen zur Antwort, dass die Informationen über den Inhalt des Grundbuches durch einen öffentlich bestellten Vermessungsingenieur aus Thüringen übermittelt worden seien. Der Name des öffentlich bestellten Vermessungsingenieurs wurde dem Grundstückseigentümer genannt.
Der betroffene Immobilienbesitzer wandte sich daraufhin an den öffentlich bestellten Vermessungsingenieur. Dieser antwortete, dass er in seiner Tätigkeit als öffentlich bestellter Vermessungsingenieur in Thüringen über den Zugang zu den Datenbanken des amtlichen Vermessungswesens gemäß § 18 Thüringer Vermessungs- und Geoinformationsgesetz (ThürVermGeoG) verfüge. Laut Aussage des Vermessungsingenieurs wurde er von der Immobilienfirma beauftragt, die Anschrift des Immobilienbesitzers zu übermitteln, da seitens der Immobilienfirma Kaufabsichten an der Immobilie des Immobilienbesitzers in Erfurt bestünden. Der öffentlich bestellte Vermessungsingenieur habe sich daraufhin im Internet über die GmbH informiert. Er fand heraus, dass die Immobilienfirma als Geschäftszweck den Erwerb von Immobilien habe und somit war für den öffentlich bestellten Vermessungsingenieur ein berechtigtes Interesse nach § 18 Abs. 2 Satz 1 ThürVermGeoG gegeben.
Die Immobilienfirma hat in der Folge aus der Liegenschaftsdatenbank die Daten zur Lage, Größe und des Eigentümers in Erfurt vom öffentlich bestellten Vermessungsingenieur erhalten. Das wollte der Immobilienbesitzer so nicht hinnehmen und wandte sich daraufhin an den

TLfDI. Der TLfDI kam in seiner rechtlichen Prüfung zu folgendem Ergebnis:
Eine Verarbeitung von personenbezogenen Daten ist nur nach Maßgabe des Art. 6 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) rechtmäßig. Personenbezogene Daten nach Art. 4 Nr. 1 DS-GVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Von dem öffentlich bestellten Vermessungsingenieur wurde die Anschrift des Eigentümers der Immobilie in Erfurt als Verantwortlicher an die Immobilienfirma übermittelt. Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Beim besagten Vermessungsingenieur handelt es sich um einen öffentlich bestellten Vermessungsingenieur in Thüringen. Er war im vorliegenden Sachverhalt Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO, da er die personenbezogenen Daten vom Immobilienbesitzer an die Immobilienfirma übermittelt hat.
Verarbeitung im Sinne der DS-GVO ist gemäß Art. 4 Nr. 2 DS-GVO jeder, mit oder ohne Hilfe automatisierter Verfahren, ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Durch die Übermittlung der Anschrift des Immobilienbesitzers an die Immobilienfirma erfolgte seitens des Vermessungsingenieurs somit eine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO.
Wie bereits erwähnt, ist eine Verarbeitung von personenbezogenen Daten nur nach Maßgabe des Art. 6 Abs. 1 DS-GVO rechtmäßig. Hierzu sind die genannten Voraussetzungen in Art. 6 Abs. 1 Satz 1

Buchstaben a) bis f) DS-GVO abzuprüfen, ob im dargestellten Sachverhalt eine zulässige Datenverarbeitung vom Verantwortlichen erfolgte beziehungsweise vorlag. Art. 6 Abs. 1 Satz 1 Buchstaben a) bis d) DS-GVO waren im konkreten Fall auszuschließen, da es hier keine Einwilligung zur oben genannten Verarbeitung vom Immobilienbesitzer gab, kein Vertragsverhältnis zwischen dem Immobilienbesitzer und dem öffentlich bestellten Vermessungsingenieur zur Übermittlung der oben genannten Daten, keine rechtliche Verpflichtung zur Datenübermittlung vom öffentlich bestellten Vermessungsingenieur für die genannten personenbezogenen Daten – und zudem war die Verarbeitung auch nicht erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Auch Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO war auszuschließen, da gemäß Art. 6 Abs. 1 Satz 2 DS-GVO Buchstabe f) nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung gilt.
Somit blieb nur noch eine Rechtgrundlage übrig: Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO ist die Verarbeitung dann rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Der öffentlich bestellte Vermessungsingenieur begründete die Datenübermittlung der Adresse des Immobilienbesitzers unter Hinweis auf § 18 Abs. 2 ThürVermGeoG. Gemäß § 18 Abs. 2 Satz 1 ThürVermGeoG stehen die Einsicht in die Namen, die Geburtsdaten und die Anschriften sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben und soweit überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden.
§ 18 Abs. 2 Satz 3 ThürVermGeoG erfordert, dass das berechtigte Interesse darzulegen ist. Der Begriff „berechtigtes Interesse“ ist hierbei ein unbestimmter Rechtsbegriff, der im Einzelfall auszulegen ist. Das berechtigte Interesse kann rechtlicher, wirtschaftlicher oder tatsächlicher Natur sein. Im Einzelfall müssen seitens des Einsichtsbegehrenden (hier der Immobilienfirma) sachliche Gründe vorgetragen werden, wodurch die Verfolgung unbefugter Zwecke oder bloße Neugier ausgeschlossen werden. Der Darlegungspflicht zum Bestehen eines berechtigten Interesses an den Angaben, wie dem vollständigen Namen und der Anschrift der Eigentümer, ist Genüge getan, wenn mit dem Verweis auf das Tätigkeitsgebiet und die Planungsabsichten dargelegt

wird, dass das Interesse der Verwirklichung wirtschaftlicher Interessen dient. Das berechtigte Interesse erfordert nach einer Entscheidung des Verwaltungsgerichts (VG) Frankfurt/Oder nicht zwingend, dass der Auskunftsbegehrende bereits in Vorverhandlungen mit dem Eigentümer steht, sondern es ist ausreichend, wenn die personenbezogenen Daten des Eigentümers erst zur Anbahnung solcher Verhandlungen beziehungsweise vorgelagert zur Klärung der Verkaufsbereitschaft des jeweiligen Eigentümers benötigt werden (vergleiche VG Frankfurt/Oder, Urteil vom 2. April 2019 – 7 K 1062/16).
Eine Beeinträchtigung des schutzwürdigen Interesses des Betroffenen war im vorliegenden Sachverhalt nicht zu erkennen, da nur berechtigte Personen, die ihr berechtigtes Interesse darlegen, Anspruch auf Auskunft aus der Datenbank des amtlichen Vermessungswesens haben. Gemäß § 18 Abs. 2 Satz 3 ThürVermGeoG ist das berechtigte Interesse darzulegen und darf nur nach § 18 Abs. 2 Satz 4 ThürVermGeoG für den Zweck genutzt werden, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt werden. Damit wird das schutzwürdige Interesse des Betroffenen gewahrt und nicht jedermann kann ohne Darlegung des berechtigten Interesses Auskünfte aus der Datenbank des amtlichen Vermessungswesens erhalten.
Die Immobilienfirma hatte sich in dem vom TLfDI zu entscheidendem Fall an den öffentlich bestellten Vermessungsingenieur gewandt, da sie aufgrund ihrer Kaufabsicht Auskunft über die Eigentümer des Grundstücks in Erfurt begehrte. Der öffentlich bestellte Vermessungsingenieur hatte sich daraufhin im Internet informiert, welchen Geschäftszweck die Immobilienfirma verfolgt. Er fand heraus, dass die Immobilienfirma als Geschäftszweck den Erwerb von Immobilien hat. Für den öffentlich bestellten Vermessungsingenieur lag aufgrund der Kaufabsicht der Immobilienfirma das berechtigte Interesse nach § 18 Abs. 2 Satz 1 ThürVermGeoG vor. Daraufhin hat er die personenbezogenen Daten (Anschrift) an die Immobilienfirma übermittelt. Die Übermittlung der personenbezogenen Daten (hier ihre Anschrift) war im Sinne des § 18 Abs. 2 Satz 1 ThürVermGeoG erforderlich. Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO hatte der öffentlich bestellte Vermessungsingenieur nach § 18 Abs. 2 Satz 1 ThürVermGeoG somit eine Rechtsgrundlage dafür, dass er die Anschrift des Immobilienbesitzers an die Immobilienfirma übermittelte.

In diesem Zusammenhang möchte der TLfDI noch auf eine andere Thematik zu sprechen kommen, die ihn während des Berichtszeitraumes beschäftigte:
Anfang des Jahres 2020 waren in Thüringen 60 Vermessungsingenieure und -ingenieurinnen öffentlich bestellt. Lediglich ein öffentlich bestellter Vermessungsingenieur hatte bis zu diesem Zeitpunkt eine/n Datenschutzbeauftragte/n bestellt, wie eine Prüfung des TLfDI aufgrund eines entsprechenden Hinweises ergab.
Der TLfDI nahm Kontakt mit allen öffentlich bestellten Vermessungsingenieuren und -ingenieurinnen sowie mit dem Thüringer Ministerium für Infrastruktur und Landwirtschaft als fachlicher Aufsichtsbehörde auf. Er teilte den Verantwortlichen mit, dass Beliehene – wie zum Beispiel öffentlich bestellte Vermessungsingenieure und –ingenieurinnen – zu den öffentlichen Stellen im Sinne des § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gehören. Gemäß Art. 37 Abs. 1 DS-GVO in Verbindung mit § 13 Abs. 1 ThürDSG bestellen öffentliche Stellen eine/n Datenschutzbeauftragte/n. Sie/Er kann ein/e Beschäftigte/r der öffentlichen Stelle sein oder ihre/seine Aufgaben auf der Grundlage eines Dienstleistungsvertrages erfüllen (§ 13 Abs. 5 ThürDSG, Art. 37 Abs. 6 DS-GVO). Es ist also auch möglich, eine/n externe/n Datenschutzbeauftragte/n zu benennen.
Die öffentlich bestellten Vermessungsingenieure und -ingenieurinnen sind daher verpflichtet, eine/n Datenschutzbeauftragte/n zu benennen sowie ihre/seine Kontaktdaten gemäß Art. 37 Abs. 7 DS-GVO zu veröffentlichen und diese Daten dem TLfDI mitzuteilen. Zweck der Veröffentlichung ist es, den betroffenen Personen zu ermöglichen, sich zur Geltendmachung ihrer Rechte an die/den Datenschutzbeauftragte/n zu wenden. Somit genügt eine einmalige Veröffentlichung (beispielsweise in der Tagespresse) nicht. Vielmehr ist ein dauerhaftes Auffinden der Angaben zur/-m Datenschutzbeauftragte/n, zum Beispiel auf der Internet-Webseite oder durch in den Büroräumen aushängende Informationen, zu gewährleisten.
Für die Meldung der Daten der/-s Datenschutzbeauftragte/n an den TLfDI steht das Online-Meldeportal unter https://tld.dsb-meldung.de zur Verfügung.
Bis Ende des Jahres 2020 hatten mit Ausnahme von zwei Verantwortlichen alle öffentlich bestellten Vermessungsingenieure und -ingenieurinnen in Thüringen eine/n Datenschutzbeauftragte/n bestellt. Sie betrauten teilweise entsprechend geschulte Mitarbeiter/innen mit die-

ser Aufgabe, teilweise wurden externe Datenschutzbeauftragte benannt.
Die beiden bisher untätig gebliebenen Vermessungsingenieure wird der TLfDI dem Thüringer Ministerium für Infrastruktur und Landwirtschaft als fachliche Aufsichtsbehörde melden und von seinen Befugnissen nach § 7 ThürDSG in Verbindung mit Art. 58 DS-GVO bei Verstößen Gebrauch machen. Ferner prüft der TLfDI die Einleitung eines Bußgeldverfahrens.
Die Veröffentlichung der Kontaktdaten hat lediglich ein weiterer Vermessungsingenieur aus gesundheitlichen Gründen bisher nicht beim TLfDI nachgewiesen. Dies wird er umgehend nachholen.

4. Fälle nicht-öffentlicher Bereich

© Praxis und Familie – Fotolia.

4.1 „Corona-Listen“

Aufgrund der Pflicht zur Kontaktdatenerfassung im Rahmen der Thüringer Verordnung zur Neuordnung der erforderlichen Maßnahmen zur Eindämmung der Ausbreitung des Corona-Virus SARS-CoV-2 sowie zur Verbesserung der infektionsschutzrechtlichen Handlungsmöglichkeiten (Corona-Verordnung) kam es thüringenweit zu Unsicherheiten bei der Umsetzung der Datenerfassungen. Teilweise wurden die Kontaktdaten nicht datenschutzkonform erhoben. Es wurden sogenannte „Corona-Listen“ geführt.

Mit der Einführung der Pflicht zur Kontaktdatenerfassung in verschiedenen Bereichen des täglichen Lebens, wie zum Beispiel in der Gastronomie oder bei Frisören und Kosmetikern, erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vermehrt Nachfragen von Verantwortlichen und auch einige Beschwerden von Betroffenen zur datenschutzkonformen Erfassung von personenbezogenen Daten.

Die Thüringer Verordnung zur Neuordnung der erforderlichen Maßnahmen zur Eindämmung der Ausbreitung des Corona-Virus SARS-CoV-2 sowie zur Verbesserung der infektionsschutzrechtlichen Handlungsmöglichkeiten (Corona-Verordnung) vom 9. Juni 2020 regelte in § 3 Abs. 4: „Zur Kontaktnachverfolgung von Gästen, Besuchern und sonstigen anwesenden Personen jeweils in geschlossenen Räumen von Gaststätten im Sinne des Thüringer Gaststättengesetzes vom 9. Oktober 2008 (GVBl. S. 367) in der jeweils geltenden Fassung oder bei öffentlichen, frei oder gegen Entgelt zugänglichen Veranstaltungen, Angeboten und Einrichtungen mit Publikumsverkehr hat die verantwortliche Person nach § 5 Abs. 2 die Kontaktdaten zu erfassen. Zu erfassen sind: Name und Vorname, Wohnanschrift oder Telefonnummer, Datum des Besuchs und Beginn und Ende der jeweiligen Anwesenheit. Die verantwortliche Person nach § 5 Abs. 2 hat die Kontaktdaten für die Dauer von vier Wochen aufzubewahren, vor unberechtigter Kenntnisnahme und dem Zugriff Dritter zu schützen, insbesondere auch durch andere Gäste oder Besucher, für die nach § 12 Abs. 1 zuständigen Behörden vorzuhalten und auf Anforderung an diese zu übermitteln sowie unverzüglich nach Ablauf der Frist nach Nummer 1 datenschutzgerecht zu löschen oder zu vernichten.“

Da die Verordnung keine weiteren Angaben hinsichtlich der Umsetzung enthielt, handhabte eine Vielzahl der verantwortlichen Unternehmen die Kontaktdatenerfassung von Gästen im Rahmen der Thüringer Verordnung, indem fortlaufende Listen ausgelegt oder erstellt wurden, in denen die betroffenen Personen ihre Kontaktdaten jeweils untereinander angeben sollten. Ein weiteres Problem bestand in der Datenerhebung an sich, da viele Verantwortliche zu viele Daten erhoben haben, die über die gesetzlich geforderten Daten hinausgingen. So wurde oftmals der Gesetzestext dahingehend verstanden, dass zwingend Adresse und Telefonnummer zu erheben seien oder auch die Angabe der E-Mail-Adresse notwendig sei.

Der TLfDI wies in solchen Fällen, wie auch in mehreren Pressemitteilungen darauf hin, dass die Kontaktdaten datenschutzkonform zu erheben sind. Das bedeutet auch, dass die Daten der Betroffenen nicht durch Dritte (also auch nicht durch sich nachfolgend eintragende Gäste) einsehbar sein dürfen. Eine Erhebung in Listenform ist daher gerade nicht zulässig gewesen! Vielmehr müssen die Daten zum Beispiel auf einzelnen Erfassungsblättern gesammelt werden.

Weiterhin ist bei der Erhebung der Daten darauf zu achten, dass auch nur die Daten erhoben werden, für die in der Corona-Verordnung auch

eine Erhebungsgrundlage besteht. Die Datenerhebung erfolgt ansonsten teilweise ohne rechtliche Grundlage und würde daher gegen Art. 5 Abs. 1 in Verbindung mit Art. 6 Abs. 1 und Art. 13 Datenschutz-Grundverordnung (DS-GVO) verstoßen. Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Art und Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die Daten müssen zudem dem Zweck angemessen und erheblich sowie auf das für die Verarbeitung notwendige Maß beschränkt sein.
Das sind nach der Corona-Verordnung nur der Name, der Vorname und daneben die Adresse oder die Telefonnummer. Eine E-Mail-Adresse oder eine Unterschrift sind nicht gefordert und dürfen daher auch nicht erhoben werden. Weiterhin müssen, wie bei jeder Datenerhebung nach der DS-GVO, Informationen nach Art. 13 DS-GVO für die Betroffenen zur Verfügung gestellt werden. Dies wurde ebenfalls in vielen Fällen missachtet.
Es war auch darauf zu achten, dass die Kontaktdaten ausschließlich zu infektionsschutzrechtlichen Zwecken verarbeitet werden und daher eine Weiterverarbeitung zu anderen Zwecken, insbesondere zu Werbe- und Vermarktungszwecken nicht erfolgen darf.
In allen dem TLfDI bekannt gewordenen Fällen und im Rahmen der vielen telefonischen Anfragen wurden die Verantwortlichen auf die bestehenden Probleme hingewiesen und bei der Umsetzung der Kontaktdatenerfassung beraten, um eine datenschutzkonforme Erfassung zu gewährleisten.
Hinsichtlich der Frage, ob eine Verordnung eine geeignete Rechtsgrundlage zur Verpflichtung der Kontaktdatenerfassung bilden kann, hat am 28. August 2020 der Verfassungsgerichtshof des Saarlandes über eine Verfassungsbeschwerde entschieden (Beschluss vom 28. August 2020 – Lv 15/20) und dabei die Vorschrift zur Kontaktnachverfolgung (§ 3 der Corona-Verordnung) für verfassungswidrig erklärt. Bei der Beschwerde ging es um verschiedene Bestimmungen der saarländischen „Verordnung zur Bekämpfung der Corona-Pandemie“ beziehungsweise der „Verordnung zur Änderung infektionsrechtlicher Verordnungen zur Bekämpfung der Corona-Pandemie vom 21. August 2020 (CP-VO)“. Im Besonderen ging es dabei auch um die Verpflichtung zur Kontaktnachverfolgung. Der Verfassungsgerichtshof des Saarlandes kam in seinem Urteil zu dem Schluss, dass über einen solchen Eingriff nicht die Exekutive alleine entscheiden dürfe:

„Das Erfordernis einer parlamentarischen gesetzlichen Grundlage ist auch keine verzichtbare bloße Formalität. Während Verordnungen wie jene zur Bekämpfung der Corona-Pandemie, bis zu ihrer Veröffentlichung im Wesentlichen im Internum der Exekutive erarbeitet, beraten und beschlossen werden, und Bürgerinnen und Bürger damit vor die vollendete und geltende Regelung gestellt werden, gewährleistet ein parlamentarisches Gesetz die Debatte von Für und Wider vor dem Forum der Öffentlichkeit und damit ein wesentliches Element der repräsentativen Demokratie. Daher mag in einer Notsituation, in denen kurzfristiges Handeln einer Regierung zwingend erscheint, die Verordnung auf der Grundlage einer hinreichend bestimmten Ermächtigung ein notwendiges und wichtiges Instrument der Staatsleitung sein. Je länger grundrechtliche Belastungen von Bürgerinnen und Bürgern indessen andauern, desto wichtiger wird es indessen, die Regelung ihrer Grundlagen und Grenzen dem ohnehin originär verantwortlichen parlamentarischen Gesetzgeber zu überlassen.“

4.2 Frage nach personalisierten Reisegutscheinen

Auch nach Inkrafttreten der DS-GVO gilt: personalisierte Reisegutscheine können verschenkt werden, wenn die Grundsätze der DS-GVO eingehalten werden. Entscheidend ist, dass ausschließlich die Daten des Beschenkten genutzt werden, die zwingend erforderlich sind, um die Reise zu buchen, dass diese Daten nur für den Vertragsschluss (Reisebuchung) genutzt werden und dass der Beschenkte über die Datenverarbeitung im Rahmen der Frist nach Art. 14 DS-GVO informiert wird.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Frage eines Reiseunternehmens, ob es noch personalisierte Reisegutscheine ausstellen dürfte. Dabei bucht ein Dritter (der Schenker) für den Beschenkten beim Reisebüro eine bestimmte Reise, übermittelt in diesem Zusammenhang die Kontaktdaten des Beschenkten an das Reisebüro, ohne dessen Einwilligung. Es stellt sich mithin die Frage, ob der Schenker die Daten des Beschenkten an das Reisebüro übermitteln darf und ob das Reisebüro diese Daten, ohne Einwilligung des Beschenkten, nutzen kann, um die Reise verbindlich für den Beschenkten zu buchen.
Der Schenker möchte in aller Regel nicht einen allgemeinen Reisegutschein verschenken, sondern eine bestimmte Reise. Zur Sicherung

verfügbarer Reiseplätze zum Zeitpunkt der Übergabe des Gutscheins ist es erforderlich, dass die Reise durch das Reisebüro gebucht wird. Dabei müssen mindestens Name, Vorname, Adresse und Geburtsdatum des künftig Reisenden verarbeitet werden, um die Reise verbindlich zu buchen.
Zunächst hat der TLfDI die Zulässigkeit der Datenverarbeitung durch das Reisebüro geprüft. Die Datenverarbeitung durch das Reisebüro ist nach Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) zulässig. Danach ist die Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Zu den berechtigten Interessen des Reisebüros zählt das wirtschaftliche Interesse an der Durchführung des Vertrages zugunsten eines Dritten (Beschenktem) zwischen dem Dritten (Schenker) und dem Reisebüro. Im Rahmen der Abwägung sind die schutzwürdigen Interessen des Betroffenen, hier das Interesse des Beschenkten, selbst zu bestimmen, wer seine personenbezogenen Daten verarbeitet, zu berücksichtigen. Im Rahmen der Interessensabwägung sind, entsprechend Erwägungsgrund 47, die vernünftigen Erwartungen der betroffenen Personen (Beschenkter) zu berücksichtigen. Entscheidend ist, ob die betroffene Person vernünftigerweise absehen kann, dass es zur Datenverarbeitung kommen wird. Einerseits hat der Betroffene (Beschenkte) zum Zeitpunkt der Datenverarbeitung keine Kenntnis von der Datenverarbeitung. Natürlich ist einem Geschenk immanent, dass der Beschenkte von den Vorkehrungen keine Kenntnis hat. Andererseits entspricht es dem weit verbreiteten Handeln, Gutscheine, auch personalisierte, ohne Einwilligung des Beschenkten zu erwerben. Dabei ist allgemein bekannt, dass bei personalisierten Gutscheinen auch personenbezogene Daten verarbeitet werden. Es muss im Rahmen der Abwägung berücksichtigt werden, dass die Daten ausschließlich zur Erfüllung des Reisevertrages verwendet werden. In diesen Grenzen ist auch, soweit es sich bei dem Reisebüro nicht selbst um einen Reiseveranstalter handelt, die Übermittlung der Daten an Dritte (Reiseveranstalter) zulässig. Die anderweitige Nutzung der Daten des Beschenkten, wie beispielsweise für Werbung, ist nicht von Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gedeckt. Auch sollten, entsprechend

dem Grundsatz der Datenminimierung, ausschließlich die Daten verarbeitet werden, die zwingend erforderlich sind, um die Reise zu buchen. Weitergehende Daten sollten erst vom Beschenkten angegeben werden.
In jedem Fall ist der Betroffene über die Datenverarbeitung entsprechend Art. 14 Abs. 1 DS-GVO zu informieren. Dabei ist die Frist entsprechend Art. 14 Abs. 3 DS-GVO zu beachten. Der Verantwortliche muss den Betroffenen unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, über die Datenverarbeitung informieren. Es handelt sich dabei um eine Höchstfrist, die nur ausgeschöpft werden darf, wenn nach den Umständen keine frühere Information geboten ist. Eine Überschreitung der Höchstfrist ist nicht zulässig (Kühling/ Buchner, Kommentar zum Datenschutz, 2. Aufl. Art. 14 Rn. 31).
Nach Art. 14 Abs. 3 Buchstabe c) DS-GVO hat die Information, falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung zu erfolgen.
Entsprechend der zuvor dargelegten Grundsätze ist auch die Datenübermittlung zwischen dem Schenker und dem Reisebüro nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zulässig. Das berechtigte Interesse des Schenkers, dem Betroffenen (Beschenktem) einen personalisierten Gutschein zu verschaffen, überwiegt in diesem speziellen Fall das schutzwürdige Interesse des Beschenkten, vorab zu wissen, an wen seine personenbezogenen Daten übermittelt werden. In jedem Fall muss auch hier der Betroffene nach Art. 14 DS-GVO nachträglich über die Datenverarbeitung informiert werden und die Daten des Beschenkten dürfen lediglich zur Vertragserfüllung genutzt werden.

4.3 Coronabedingte Gutscheine bei Absagen von Veranstaltungen – Wann bekommt man dennoch Geld ausgezahlt? (Überprüfung persönlicher Lebensumstände)

Werden Veranstaltungen aufgrund der Corona-Pandemie abgesagt, wird dem Betroffenen in der Regel ein Gutschein beim Veranstalter ausgestellt. Möchte der Betroffene jedoch nicht den Gutschein, sondern den Kaufpreis erstattet bekommen, muss er einen Nachweis über seine prekären Lebensumstände erbringen.

Im Berichtszeitraum wandte sich ein Betroffener an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und fragte, ob er bereits geleistete Zahlungen für ein Ticket erstattet bekäme. Dem Betroffenen wurde seitens des verantwortlichen Veranstalters mitgeteilt, dass er einen Nachweis über seine prekären Lebensumstände erbringen müsste. Andernfalls bekäme er lediglich einen Gutschein für die Veranstaltung ausgestellt.
Zur Abfederung der Auswirkungen der seitens der Bundesregierung und der Regierungen der Länder beschlossenen Absage aller Großveranstaltungen wurde ein Gesetz erlassen, wonach die Sport- und Konzertveranstalter dem Kunden statt der Auszahlung des Ticketpreises einen Gutschein ausstellen durften.
Danach gilt laut (Art. 240 § 5 Abs. 5 Nr. 1 Einführungsgesetz zum Bürgerlichen Gesetzbuch [EGBGB]) *Folgendes:*
(1) Wenn eine Musik-, Kultur-, Sport- oder sonstige Freizeitveranstaltung aufgrund der COVID-19-Pandemie nicht stattfinden konnte oder kann, ist der Veranstalter berechtigt, dem Inhaber einer vor dem 8. März 2020 erworbenen Eintrittskarte oder sonstigen Teilnahmeberechtigung anstelle einer Erstattung des Eintrittspreises oder sonstigen Entgelts einen Gutschein zu übergeben. Umfasst eine solche Eintrittskarte oder sonstige Berechtigung die Teilnahme an mehreren Freizeitveranstaltungen und konnte oder kann nur ein Teil dieser Veranstaltungen stattfinden, ist der Veranstalter berechtigt, dem Inhaber einen Gutschein in Höhe des Wertes des nicht genutzten Teils zu übergeben.
(2) Soweit eine Musik-, Kultur-, Sport- oder sonstige Freizeiteinrichtung aufgrund der COVID-19-Pandemie zu schließen war oder ist, ist der Betreiber berechtigt, dem Inhaber einer vor dem 8. März 2020 erworbenen Nutzungsberechtigung anstelle einer Erstattung des Entgelts einen Gutschein zu übergeben.
(3) Der Wert des Gutscheins muss den gesamten Eintrittspreis oder das gesamte sonstige Entgelt einschließlich etwaiger Vorverkaufsgebühren umfassen. Für die Ausstellung und Übersendung des Gutscheins dürfen keine Kosten in Rechnung gestellt werden.
(4) Aus dem Gutschein muss sich ergeben,
1. dass dieser wegen der COVID-19-Pandemie ausgestellt wurde und
2. dass der Inhaber des Gutscheins die Auszahlung des Wertes des Gutscheins unter einer der in Absatz 5 genannten Voraussetzungen verlangen kann.

(5) Der Inhaber eines nach den Absätzen 1 oder 2 ausgestellten Gutscheins kann von dem Veranstalter oder Betreiber die Auszahlung des Wertes des Gutscheins verlangen, wenn
1. der Verweis auf einen Gutschein für ihn angesichts seiner persönlichen Lebensumstände unzumutbar ist oder
2. er den Gutschein bis zum 31. Dezember 2021 nicht eingelöst hat.

Dabei handelt es sich um eine zivilrechtliche Norm, mit der der Gesetzgeber die Auszahlungsvoraussetzungen in solchen Fällen wie dem des Betroffenen geregelt hat.

Die Datenverarbeitung durch den verantwortlichen Veranstalter in diesem Zusammenhang beruht auf Art. 6 Abs. 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO). Danach ist die Verarbeitung zulässig für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen. Dies betrifft insbesondere die personenbezogenen Daten, die zur Erfüllung der Hauptpflichten eines Vertrages oder zur Beendigung des Vertrages erforderlich sind.

Hier geht es im Folgenden um die Frage der Zulässigkeit der Modifizierung der Hauptleistung (statt Ticket zu einer bestimmten Veranstaltung erhält der Käufer einen Gutschein) und die Frage nach der Zulässigkeit der Rückzahlung der Leistung des Käufers. Dabei sollen weitere personenbezogene Daten des betroffenen Käufers verarbeitet werden, damit der verantwortliche Verkäufer das Vorliegen seiner Rückzahlungsverpflichtung überprüfen kann.

Der Gesetzgeber hat zur Abfederung der Folgen der Corona-Pandemie für Veranstalter die oben dargestellten Regelungen zur Rückabwicklung von ausgefallenen Veranstaltungen aufgrund der Corona-Pandemie erlassen. Im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO stellt sich die Frage, ob nun weitere personenbezogene Daten des Betroffenen verlangt werden können, um den Rückzahlungsanspruch aus Art. 240 § 5 Abs. 5 Nr. 1 EGBGB geltend machen zu können. Dabei sind allgemeine zivilrechtliche Überlegungen zu berücksichtigen. So muss derjenige, der einen Anspruch durchsetzen will (Rückzahlung des Kaufpreises), dessen Voraussetzungen auch beweisen. Spätestens im Rahmen eines Zivilprozesses müssen dann die entsprechenden Umstände dargelegt und unter Beweis gestellt und somit dem Verantwortlichen offenbart werden. Daher können die Daten zur Anspruchsprüfung durch den verantwortlichen Veranstalter auch bereits vor Beginn eines Zivilprozesses verarbeitet werden.

Im Ergebnis werden personenbezogene Daten zur Erfüllung eines Vertrages im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO zulässigerweise verarbeitet.
Zudem kann die Verarbeitung personenbezogener Daten im Rahmen der Rückabwicklung von Ticketkäufen auf Grundlage des Art. 240 § 5 EGBGB auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden. Danach ist die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.
Zum berechtigten Interesse des verantwortlichen Veranstalters zählt hier das Interesse, das Vorliegen einer Auszahlungsverpflichtung zu überprüfen, soweit sich ein Betroffener auf die Rückzahlungsklausel nach Art. 240 § 5 Abs. 5 Nr. 1 EGBGB beruft. Das schutzwürdige Interesse des Betroffenen umfasst sein Interesse, eigene Angaben zu prekären Lebensumständen gegenüber Dritten zu vermeiden. Hier begehrt der Betroffene die Rückzahlung eines Veranstaltungstickets. Im Rahmen der Abwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO ist zu berücksichtigen, dass für diesen Rückzahlungsanspruch besondere Voraussetzungen bestehen, die in Art. 240 § 5 EGBGB geregelt sind.
Im Übrigen gelten die allgemeinen Grundsätze der DS-GVO. Die Daten dürfen vom Verantwortlichen nur zu dem Zweck „Prüfung der Unzumutbarkeit bezüglich der Rückzahlung des Ticketpreises aufgrund der persönlichen Lebensumstände“ verarbeitet werden. Danach müssen im Sinne der Datensparsamkeit nach Art. 5 Abs. 1 Buchstabe c) DS-GVO sofort nach Abschluss der Entscheidung über die Rückzahlung des Ticketpreises alle personenbezogenen Daten gelöscht werden.
Zudem hat der TLfDI darauf hingewiesen, dass im Rahmen der „persönlichen Lebensumstände“ nicht ausschließlich Umstände wie Kurzarbeit und Kündigung Einfluss haben. Auch personenbezogene Daten zu den Fragen, ob ein sehr weiter Anreiseweg zum Veranstaltungsort vorlag oder ob Veranstaltungen im Rahmen einer ebenfalls abgesagten Reise betroffen sind, dürften verarbeitet werden (vergleiche auch Bundesministerium der Justiz und für Verbraucherschutz: Fragen und Antworten: Gutscheinlösung bei Veranstaltungsverträgen – Veranstaltungsvertragsrecht; abrufbar unter:

https://www.bmjv.de/DE/Themen/FokusThemen/Corona/Tickets/FAQ_Gutscheine.pdf?__blob=publicationFile&v=2).

4.4 Wahlwerbung durch Versicherungsmakler (Verwarnung)

Die personenbezogenen Daten einer betroffenen Person, die im Rahmen privater oder geschäftlicher Beziehungen erhoben wurden, sind ohne eine Einwilligung und eine Information über die beabsichtigte Zweckänderung nach Art. 13 Abs. 2 DS-GVO nicht für die Versendung von Wahlwerbung des Verantwortlichen nutzbar. Es handelt sich hierbei um eine rechtswidrige Verwendung der personenbezogenen Daten.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen einer Beschwerde bekannt, dass ein als Makler tätiger Verantwortlicher die Namen und Adressen von betroffenen Personen (Kunden), welche er aus seiner Tätigkeit als Makler erhalten hatte, für die Übersendung von Wahlwerbung genutzt hat. In dem Werbeschreiben, welches an die betroffenen Personen gesendet wurde, wurde auf die geschäftliche Beziehung ausdrücklich Bezug genommen.
Daraufhin reichte ein Betroffener eine Beschwerde beim TLfDI ein. Der TLfDI hat den Makler daraufhin angehört und um Stellungnahme gebeten. Der Verantwortliche antwortete, dass er zu Zwecken des privaten Wahlkampfes alle privaten Kontakte per Brief angeschrieben und kontaktiert habe. Dazu würden auch Bekannte zählen, mit denen er auch geschäftlich zusammenarbeite.
Zunächst war festzustellen, dass die Datenschutz-Grundverordnung (DS-GVO) anwendbar ist. Eine Ausnahme vom Anwendungsbereich liegt nur dann vor, wenn personenbezogene Daten von natürlichen Personen verarbeitet werden zur Ausübung ausschließlich persönlicher oder familiärer Zwecke. Diese Ausnahmeregelung ist restriktiv anzuwenden. Nach Erwägungsgrund 18 ist Abgrenzungskriterium das Fehlen jeglichen Bezugs zu einer beruflichen oder wirtschaftlichen Tätigkeit, das bedeutet, dass keinerlei geschäftlicher Bezug erkennbar sein darf. Dies ist vorliegend aber gerade nicht der Fall gewesen. Der Makler hat angegeben, zu allen genutzten privaten Kontakten auch geschäftliche Beziehungen zu haben. Weiterhin zählt auch die Wahlwerbung im Rahmen einer Kommunalwahl nicht zur Ausübung rein persönlicher oder familiärer Tätigkeiten. Weiterhin hat sich der Verant-

wortliche in dem Anschreiben ausdrücklich auf die geschäftlichen Beziehungen bezogen. Die DS-GVO war daher anwendbar.
Mit Versendung des Werbeschreibens an die betroffenen Personen kam es zur Verarbeitung von personenbezogenen Daten insbesondere des Namens und der Postadresse der Betroffenen. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen sind, identifiziert werden kann“. Eine Identifizierung ist somit möglich. Das Zusenden des Werbeschreibens stellt eine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO dar. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
Es liegt zunächst ein Verstoß gegen Art. 5 Abs. 1 Buchstabe a) und Buchstabe b) DS-GVO vor. Diese besagen, dass personenbezogene Daten auf rechtmäßige Art und Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Weiterhin müssen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Gemäß Art. 6 Abs. 1 DS-GVO ist eine Verarbeitung nur dann rechtmäßig, wenn eine der Bedingungen der Buchstaben a) bis f) vorliegen, das heißt, wenn es eine rechtliche Grundlage für die Datenverarbeitung gibt.
Eine Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a) DS-GVO der angeschriebenen Personen zur werblichen Ansprache liegt nicht vor. Eine vertragliche Grundlage gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist ebenfalls auszuschließen. Ein berechtigtes Interesse gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO ist jedes Interesse des Verantwortlichen, egal ob wirtschaftlicher rechtlicher oder ideeller Art. Doch auch wenn man zu Gunsten des Verantwortlichen ein derartiges Interesse annehmen würde, wiegt das schützenswerte Interesse des Betroffenen in dem Falle höher. Die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortli-

chen beruhen, sind zu berücksichtigen. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen. Der Betroffene muss nicht damit rechnen, dass er mit Wahlwerbung von Personen angesprochen wird, mit denen er geschäftlichen oder privaten Umgang pflegt. Die personenbezogenen Daten der betroffenen Personen wurden ursprünglich auch nicht für Zwecke der Wahlwerbung erhoben. Die Erhebung erfolgte in diesem Fall wegen einer Vermietung. Die Verwendung dieser Daten für die Übersendung von Wahlwerbung ist keine mit dem Erhebungszweck zu vereinbarende Art und Weise.
Gemäß Art. 13 Abs. 3 DS-GVO muss der Verantwortliche, wenn er beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, als den, für den sie erhoben worden sind, der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen Zweck und alle maßgeblichen Informationen nach Art. 13 Abs. 2 DS-GVO zur Verfügung stellen. Dem Werbeschreiben gingen keine Informationen an die betroffene Person voraus oder waren dem Schreiben beigefügt. Dies stellt einen Verstoß gegen den Transparenzgrundsatz aus Art. 5 Abs. 1 Buchstabe a) DS-GVO dar. Der Verantwortliche wurde daraufhin vom TLfDI gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt.

4.5 Beschwerde über einen Rechtsanwalt wegen Datenweitergabe ohne Einwilligung

Personenbezogene Daten dürfen nur auf rechtmäßige, für die betroffene Person nachvollziehbare, Weise verarbeitet werden. Für eine rechtmäßige Verarbeitung muss entweder eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO oder eine anderweitige Rechtsgrundlage für eine Verarbeitung vorliegen. Die erteilte Einwilligung muss dabei auch nachweisbar sein.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen einer Beschwerde bekannt, dass ein Rechtsanwalt personenbezogene Daten verarbeitet beziehungsweise an Dritte übermittelt haben soll, ohne hierfür berechtigt gewesen zu sein, indem er Informationen über den Stand eines Gerichtsverfahrens seines Mandanten an einen Dritten weitergegeben hat.

Ein Mandant beschwerte sich beim TLfDI, nachdem er einen Rechtsanwalt aufgesucht hatte und dort mit seinem Bruder zusammen den Besprechungstermin mit dem Anwalt wahrgenommen hatte. In diesem Besprechungstermin wurde das weitere gerichtliche Vorgehen besprochen. Etwaige Einwände gegen eine Mitteilung auch gegenüber dem Bruder wurden zu diesem Zeitpunkt von dem Mandanten nicht vorgetragen, weshalb das umfangreiche Beratungsgespräch im Beisein des Bruders weitergeführt wurde.
Als der Bruder zu einem späteren Zeitpunkt in einer eigenen Angelegenheit bei demselben Rechtsanwalt einen Termin wahrnahm, wurden ihm auf Nachfrage Auskünfte über den Verfahrensstand des anderen Verfahrens gegeben, was nach Ansicht des Mandanten einen Verstoß darstellt. Bei der Prüfung dieses Falles ist zu beachten, dass der TLfDI für die Prüfung der Einhaltung etwaiger standesrechtlicher Normen durch Rechtsanwälte nicht zuständig ist und die Prüfung daher unter rein datenschutzrechtlichen Aspekten erfolgte.
Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen an den Rechtsanwalt, um den Sachverhalt näher aufzuklären. Nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 Satz 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung rechtmäßig ist. Es handelt sich somit um ein so genanntes Verbot mit Erlaubnisvorbehalt.
Eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO durch den Betroffenen hinsichtlich der Übermittlung seiner personenbezogenen Daten in Form von Auskünften über den Verfahrensstand lag nicht vor. Eine Einwilligung ist jede freiwillige für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, Art. 2 Nr. 11 DS-GVO. Gemäß Art. 7 Abs. 1 DS-GVO muss der Verantwortliche zudem nachweisen können, dass die betroffene Person in die Verarbeitung, hier die Übermittlung an einen Dritten, ihrer personenbezogenen Daten eingewilligt hat. Einen derartigen Nachweis konnte der Anwalt jedoch nicht führen, da die Einwilligung im Beratungsgespräch nicht schriftlich eingeholt wurde und vom Mandanten auch nicht bestätigt wurde. Die Befugnis zur Übermittlung der Auskünfte kann auch nicht auf

Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden. Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO dann rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Es ist schon fraglich, ob für den verantwortlichen Anwalt ein berechtigtes Interesse daran besteht, den Bruder seines Mandanten über den Verfahrensstand in Kenntnis zu setzen. Die Erforderlichkeit zur Wahrung der berechtigten Interessen richtet sich danach, ob andere gleich effektive, aber für den Mandanten als betroffene Person weniger beeinträchtigende Mittel zur Verfügung standen. Insoweit wäre es das mildere Mittel gewesen, die Information über den Verfahrensstand direkt an den Mandanten zu geben, da in diesen Fall auch keine Dringlichkeit oder ähnliches bestand.
Der Rechtsanwalt war nicht befugt, Auskünfte über den Verfahrensstand an den Bruder seines Mandanten zu übermitteln, auch wenn dieser vorher bei einem Beratungsgespräch zugegen gewesen ist. Der Rechtsanwalt wurde aus diesem Grund vom TLfDI gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt und es wurde ihm für die zukünftige Handhabung empfohlen, derartige datenschutzrechtliche Einwilligungen zur Weitergabe an Dritte schriftlich vom Mandanten einzuholen, damit er als Verantwortlicher seine dahingehende Nachweispflicht aus Art. 7 Abs. 1 DS-GVO in jedem Fall erfüllen kann. Hierbei ist noch zu beachten, dass die Einwilligung in informierter Weise zu erfolgen hat und auch den Hinweis auf die jederzeitige Widerrufsmöglichkeit enthalten muss.

4.6 Aufforderungs-E-Mails zur Bewertung eines Online-Shops bedürfen der Einwilligung des Betroffenen

Die Versendung einer E-Mail zum Zwecke der Aufforderung um Bewertung des vorher durch den Betroffenen genutzten Online-Shops stellt einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO dar, solange dafür keine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO vorliegt.

Ein Thüringer Unternehmen, welches auch einen Online-Shop betreibt, hat einem Kunden nach Abschluss eines Onlinekaufes eine E-Mail mit der Aufforderung zur Bewertung des Online-Shops zuge-

sandt. Als Zweck dieser E-Mail wurden die Analyse und Verbesserung des Online-Shops angegeben. Der Kunde hat im Rahmen seines Kaufgeschäftes dazu keinerlei Einwilligungen abgegeben. Der betroffene Kunde legte Beschwerde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein.
Bei der Aufforderung zur Bewertung eines Shops handelt es sich um eine Werbemaßnahme. Werbung wird definiert als „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern“ (Art. 2 Buchstabe a) der EU-Richtlinie 2006/114/EG über irreführende und vergleichende Werbung vom 12. Dezember 2006).
Eine Rechtsgrundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung findet sich in der Datenschutz-Grundverordnung (DS-GVO), abgesehen von einer Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, nur in Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen. Anhaltspunkte für die zu treffende Abwägungsentscheidung enthält Erwägungsgrund 47 DS-GVO, der unter anderem ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“
In diesem Fall wäre eine Datenverarbeitung aufgrund eines berechtigten Interesses des Verantwortlichen möglicherweise gerechtfertigt, wenn sie erforderlich wäre, um ein berechtigtes wirtschaftliches Interesse des Verantwortlichen zu wahren und keine schutzwürdigen Interessen der Betroffenen höher gewichtet werden müssen. Zur Förderung des Produktabsatzes ist es grundsätzlich ein legitimes wirtschaftliches Interesse des Verantwortlichen, Werbemaßnahmen durchzuführen.
Vorliegend handelte es sich aber aufgrund des Kontaktweges per E-Mail um eine im Rahmen der Bewertung der Zulässigkeit zu berücksichtigende Besonderheit. Hierzu regelt das Wettbewerbsrecht in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist. Weil Art. 6 Abs. 1

Satz 1 Buchstabe f) DS-GVO eine Verarbeitung personenbezogener Daten nur für zulässig erklärt, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sind auch bei der datenschutzrechtlichen Beurteilung einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung, die Wertungen in den Schutzvorschriften des UWG für die jeweilige Werbeform mit zu berücksichtigen. Wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person danach nicht erlaubt ist, kann die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO auch nicht zugunsten der Zulässigkeit einer Verarbeitung dieser Kontaktdaten für Zwecke der Direktwerbung ausfallen. (Siehe dazu auch Orientierungshilfe Direktwerbung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf).

Die Werbung per E-Mail stellt eine unzumutbare Belästigung im Sinne des § 7 Abs. 1 UWG dar, da nach § 7 Abs. 2 Nr. 3 UWG eine Werbung unter Verwendung elektronischer Post ohne vorherige ausdrückliche Einwilligung des Adressaten vorliegt. Es greift auch nicht die Privilegierung des § 7 Abs. 3 UWG, der hiervon abweichend regelt, dass bei Vorliegen der dort genannten Voraussetzungen keine unzumutbare Belästigung vorliegt, da die Werbung auch nicht für eigene ähnliche Waren oder Dienstleistungen des Verantwortlichen erfolgte. Eine Zufriedenheitsabfrage per E-Mail nach einem Onlineverkauf dient nur der Verbesserung des Online-Shops und ist für das weitere Bewerben von Produkten nicht erforderlich.

Demzufolge ist die Zusendung einer solchen Bewertungs-E-Mail nur über den Tatbestand der Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO zu rechtfertigen. Eine solche wurde allerdings vom Unternehmen im Rahmen des Kaufvorgangs nicht abgefordert, sodass das Handeln des Unternehmens einen Datenschutzverstoß darstellt. Der TLfDI hat nach Anhörung des verantwortlichen Unternehmens diesem gegenüber eine Verwarnung im Verwaltungsverfahren ausgesprochen. Gleichzeitig hat das verantwortliche Unternehmen eine technische Umstellung vorgenommen. Die Versendung von derartigen Bewertungs-E-Mails erfolgt nun nur noch nach ausdrücklicher Einwilligung des Kunden, sodass ein gesetzeskonformer Zustand geschaffen wurde.

4.7 WhatsApp-Adressdaten kontrollieren – über die Möglichkeiten von WhatsBox

WhatsApp in seiner Standardinstallation überträgt regelmäßig die Telefonbucheinträge an Server von WhatsApp. Wer vorher keine Einwilligung von Bürgern der Telefonbucheinträge eingeholt hat, begeht somit einen Datenschutzverstoß, wenn diese gar keine WhatsApp-Nutzer sind. Für Android-Nutzer kann hier Abhilfe durch die App „WhatsBox“ geschaffen werden, da dann die Daten der Nutzer, welche ihre Einwilligung gegeben haben oder bereits WhatsApp-Nutzer sind, in ein separates Telefonbuch übernommen werden können, welches dann an WhatsApp übertragen wird.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete bereits in seinem Tätigkeitsbericht von 2018 in Nummer 5.35 über die datenschutzrechtlichen Bedenken bei der Nutzung von WhatsApp. Problematisch ist aus Sicht des TLfDI weiterhin, dass auch Kontaktdaten (Telefonnummern) von Nicht-WhatsApp-Mitgliedern aus dem Kontaktbereich des Gerätes ausgelesen werden, wofür es keine Einwilligung der betroffenen Personen gibt. Auch nach zwei Jahren hat sich bei WhatsApp durch Facebook diesbezüglich nichts getan – hier musste also ein Drittherstellen tätig werden. Zudem kann WhatsApp nachverfolgen, welche Nutzer mit welchen anderen Nutzern wie häufig kommunizieren und welche Art von Inhalten verschickt wird (auch verschlüsselte Daten können klassifiziert werden, ob es Fotos, Videos, Audiodateien oder einfach nur Textnachrichten sind, siehe zum Beispiel https://arxiv.org/abs/1905.11873).
Daher wurde im Jahr 2018 für Android-Systeme die App „WhatsBox“ von der SRT GmbH entwickelt, welche die Einwilligungsproblematik handhabbarer machen soll. So fungiert die App als ein zusätzlicher Datencontainer, in welchem eine separate Instanz von WhatsApp installiert wird. In dem Container wird ein zweites Adressbuch angelegt, welches mit den Adressen (als Kopie) gefüllt werden kann. So kann ein Nutzer die Kontakte, für welche auch eine Einwilligung zur Datenübertragung an WhatsApp vorliegt beziehungsweise auch die Daten von Nutzern, die schon WhatsApp nutzen, dort abspeichern. Ist die App installiert, greift WhatsApp nur noch auf den Datencontainer und nicht mehr auf das zentrale Telefonbuch zu.

Unter Nutzung von „WhatsBox“ ist es also möglich, die rechtlich notwendigen Einwilligungserfordernisse auch praktikabel umzusetzen. Insoweit ist das Prinzip plausibel und es kann davon ausgegangen werden, dass somit auch ein wirksamer Schutz der Kontaktdaten hergestellt werden kann. Es gilt allerdings zu beachten, dass es sich bei der „WhatsBox“ um eine App-in-der-App handelt. Diese App ist nur im Container sichtbar und kann auch nur dann gestartet werden, wenn „WhatsBox“ gestartet wird. Auch muss die App „WhatsBox“ dann im Hintergrund aktiv bleiben, um die im Container integrierte App „WhatsApp“ als Hintergrunddienst laufen zu lassen. Ist WhatsApp außerhalb von „WhatsBox“ installiert, kann der Filtermechanismus der Kontaktdaten nicht wirksam werden. Daher muss „WhatsApp“ außerhalb von „WhatsBox“ deinstalliert werden, da sonst nach wie vor die Weiterleitung des gesamten Adressbuchs erfolgt.
Vom TLfDI wurde nicht geprüft, inwieweit die App „WhatsBox“ vertrauensvoll mit den Adressdaten des Adressbuches umgeht. Die App selber hat weitreichende Systemrechte und selber vollen Zugriff auf das Adressbuch (und weitere Dateibereiche des Smartphones). Unter den Nutzerbewertungen der App im Google-App-Store sind einige Fehlerberichte zu finden (siehe https://play.google.com/store/apps/details?id=de.backessrt.wb&hl=de). Bei Fehlfunktion der Adressbuchsynchronisation in den Container hinein kann dadurch vom Nutzer unbeabsichtigt eine unrechtmäßige Datenübermittlung an WhatsApp ausgelöst werden. Ein gewisses Restrisiko für eine Fehlfunktion der App „WhatsBox“ existiert also, kann aber auch bei keiner anderen Software ausgeschlossen werden. Es gilt dennoch aus Sicht des TLfDI, dass die Nutzung der App datenschutzgerechter ist als WhatsApp in seiner ursprünglichen Version. Leider gilt dies nur für Android-Endgeräte.
Auch wenn die irische Datenschutzaufsichtsbehörde federführend für WhatsApp zuständig ist, wird der TLfDI weiterhin das Thema im Blick behalten, um Sie beraten zu können.

4.8 Daten von Betreuten auf Abwegen

Die Weitergabe von personenbezogenen Daten betreuter Personen an unberechtigte Dritte über einen versehentlich genutzten E-Mail-Verteiler stellt eine unzulässige Übermittlung von personenbezogenen Daten dar, da keine Rechtsgrundlage die Verarbeitung rechtfertigt.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde über einen Betreuungsverein, der personenbezogene Daten von betreuten Personen an mehrere unberechtigte Empfänger per E-Mail weitergeleitet hatte. Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen an den Verantwortlichen. Es konnte daraufhin festgestellt werden, dass unter anderem der Vor- und Nachname von betreuten Personen, Aktenzeichen des Betreuungsgerichts sowie Ort des Betreuungsgerichts und Rechnungsbeträge an insgesamt zehn unberechtigte Empfänger übermittelt wurden. Der Verantwortliche hatte hier aus Versehen eine Verteilerfunktion genutzt. Unmittelbar nach Bemerken des Fehlers hatte er die Empfänger über die fehlgeleitete E-Mail informiert und um Löschung dieser gebeten.
Trotz des unmittelbaren Feststellens des Fehlers liegt in diesem Fall eine Übermittlung von personenbezogenen Daten im Sinne des Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) vor. Die Daten wurden den Empfängern so zugänglich gemacht, dass sie Kenntnis vom Informationsgehalt der betreffenden Daten erlangen können. Zudem handelt es sich bei den personenbezogenen Daten der Betreuten um, wenn auch mittelbar, besondere Kategorien personenbezogener Daten, da durch den Umstand, dass eine Betreuung für diese Person gegeben ist, Rückschlüsse auf deren geistigen beziehungsweise körperlichen Gesundheitszustand geschlossen werden können, Art. 9 Abs. 1 DS-GVO.
Eine Verarbeitung muss auf rechtmäßige Weise erfolgen, das heißt, eine Rechtsgrundlage muss die vorgenommene Verarbeitung rechtfertigen. Im Rahmen der DS-GVO sind hier die Rechtmäßigkeitstatbestände des Art. 6 Abs. 1 Satz 1 DS-GVO zu prüfen. Eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a), 7 DS-GVO lag seitens der betreuten Personen nicht vor. Auch auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO kann die erfolgte Verarbeitung nicht gestützt werden. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Es fehlt bereits an einem berechtigten Interesse des Verantwortlichen, die personenbezogenen Daten der betreuten Personen an die falschen Personen zu übermitteln. Aus diesem Grund überwiegen bereits die Interessen der betroffenen Personen. Ferner handelt es sich bei den hier übermit-

telten Daten zumindest mittelbar um besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, was den Eingriff in die Rechte der betroffenen Personen verstärkt. Zudem ist die Verarbeitung von besonderen Kategorien personenbezogener Daten nur unter den Voraussetzungen des Art. 9 Abs. 2 Buchstabe a) bis j) DS-GVO zulässig. Da keine Einwilligung der betreuten Personen in die Übermittlung vorlag und auch die sonstigen Voraussetzungen des Art. 9 Abs. 2 DS-GVO nicht gegeben waren, lag insoweit auch keine rechtmäßige Übermittlung von besonderen Kategorien personenbezogener Daten vor.
Der verantwortliche Verein wurde seitens des TLfDI nach Art. 58 Abs. 2 Buchstabe b) DS-GVO mittels kostenpflichtigen Bescheides verwarnt.

4.9 Beschwerde über offenen E-Mail-Verteiler

Verantwortliche müssen dafür Sorge tragen, dass personenbezogene E-Mail-Adressen nicht unbefugt Dritten zur Kenntnis gegeben werden. Hierfür kann die BCC-Funktion in der E-Mail genutzt werden.

Immer wieder erhält der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Kenntnis von Fällen, in denen Verantwortliche E-Mails an eine Vielzahl von Empfängern in einer Art und Weise aussenden, dass sämtliche E-Mail-Adressen für alle Empfänger der E-Mail sichtbar waren. Vielmals geschieht dies unwissend in der Funktion des E-Mail-Clients. Die E-Mail-Adressen werden häufig in das „AN-Feld“ eingetragen, wodurch jeder Empfänger sehen kann, wer diese E-Mail bekommen hat.
Die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ist nur zulässig, wenn dafür eine gesetzliche Grundlage oder eine Einwilligung der betroffenen Personen vorliegt. Die Verantwortlichen haben dafür Sorge zu tragen, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes unbefugter oder unrechtmäßiger Verarbeitung, Art. 5 Abs. 1 Buchstabe f) DS-GVO. Dazu sind geeignete technische und organisatorische Maßnahmen wahrzunehmen, um sicherzustellen, dass eine Verarbeitung personenbezogener Daten gemäß der DS-GVO erfolgt.
Bei vielen E-Mail-Adressen handelt es sich um solche, die den Vor- und Nachnamen beinhalten. Für die Übermittlung der E-Mail-Adres-

sen an die jeweiligen Empfänger war in den bearbeiteten Fällen keine Rechtsgrundlage gegeben. Hierbei mangelt es offenbar an der Kenntnis der Funktion des E-Mail-Clients. Statt in das „AN-Feld“ oder „CC-Feld“ sind die E-Mail-Adressen in das „BCC-Feld“ einzutragen. Denn nur bei dieser Eintragung wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, so dass keiner erkennen kann, an wen diese E-Mail noch versandt wurde.
Der Umstand, dass E-Mail-Adressen von betroffenen Personen auf solchen offenen E-Mail-Verteilern für alle Personen sichtbar sind, kann ein Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellen, weshalb die Verantwortlichen auf die datenschutzkonforme Verwendung der Funktionen der E-Mail-Clients hingewiesen wurden.

4.10 Ja, wo ist er denn...? Patient im Klinikum unauffindbar – wenn das elektronische Krankenhausinformationssystem Rätsel aufgibt

Personenbezogene Daten nach Art. 5 Abs. 1 Buchstabe d) DS-GVO müssen „sachlich richtig und […] auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)“. Diese Vorgabe gilt auch für das personenbezogene Datum über den physischen Vitalzustand einer Person („leben“ oder „verstorben“).

Ende Juli 2019 fand sich in einer Thüringer Tageszeitung ein Artikel mit der Überschrift „Verschollen im […] Klinikum“. Diese Schlagzeile veranlasste den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), dem Sachverhalt nachzugehen.
Gesundheitsdaten gehören nach Art. 9 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) zu den sogenannten besonderen Datenkategorien, die einem erhöhten Schutz unterliegen. Dies gilt auch und ganz besonders für den Umgang mit digitalen Patientenakten im elektronischen Krankenhausinformationssystem (KIS). Ein datenschutzkonformes Rollen- und Rechtekonzept für Zugriffe von Krankenhausmitarbeitern auf Patientenakten muss technisch so gestaltet sein, dass jeder Mitarbeiter nur über Zugriffsrechte für „seinen“ medizinischen Anwenderbereich (beispielsweise „Pflege“) in seinem eigenen klinischen Fach-

bereich beziehungsweise auf „seiner“ Station verfügt. Die Orientierungshilfe Krankenhausinformationssystem der Arbeitskreise Gesundheit und Soziales sowie technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder enthält klare Regeln über die Rollen- und Rechtekonzepte für den Zugriff auf Patientendaten im KIS, die datenschutzrechtlich zwingend einzuhalten sind. Nach Art. 32 DS-GVO muss der Verantwortliche alle technischen und organisatorischen Maßnahmen ergreifen, um ein angemessenes Schutzniveau bei der Verarbeitung von personenbezogenen (Gesundheits-)Daten zu gewährleisten.
Durch das Ereignis, das sich hinter der Zeitungsschlagzeile vom Juli 2019 verbarg, wurde deutlich, dass diese technischen und organisatorischen Maßnahmen im in Rede stehenden Krankenhaus nicht ausreichend waren, um die Integrität von Patientendaten zu wahren beziehungsweise zu schützen. Besonders bei Daten von Patienten, die keine Angehörigen (mehr) haben, sondern einen gesetzlichen Betreuer oder bei Patienten, die aus einem Seniorenheim ins Klinikum eingeliefert werden, ist dieser Aspekt aus Sicht des Datenschutzes besonders kritisch.
Im Mai 2019 war der Bewohner eines Seniorenheims aufgrund von Herzbeschwerden in das Klinikum eingeliefert worden. Bereits im Seniorenheim war der Patient regelmäßig physiotherapeutisch betreut worden. Sofern es der gesundheitliche Zustand des Patienten zuließ, sollte die Physiotherapie auch im Klinikum fortgesetzt werden. Daher begab sich die Physiotherapeutin nach vier Tagen ins Klinikum, um sich nach dem Gesundheitszustand des Patienten zu erkundigen. Im Klinikum wurde ihr mitgeteilt, dass sich der Patient auf der kardiologischen Station befinde, aber gegenwärtig bei einer medizinischen Untersuchung sei. Die Physiotherapeutin gab diese Information an die Leiterin des Seniorenheims weiter. In den Folgetagen erkundigte sich die Leiterin des Seniorenheimes wiederholt im Klinikum nach dem gesundheitlichen Befinden des Heimbewohners, damit gegebenenfalls seine physiotherapeutische Behandlung fortgesetzt werden könnte. Jedoch erhielt die Leiterin des Seniorenheims bei jedem Anruf unterschiedliche und sich zum Teil widersprechende Auskünfte: der Patient befinde sich auf der kardiologischen Station, nehme aber gerade an einer Reha-Maßnahme teil, der Patient befinde sich jetzt auf der Diabetes-Station, aber es könne nicht gesagt werden, ob der Patient gerade im Zimmer ist, man wüsste nicht, auf welcher Station sich der Patient zur Zeit befinde… Schlussendlich erhielt die Leiterin des

Seniorenheims die Auskunft, dass sich ein Patient des genannten Namens gar nicht im Klinikum befände. Daraufhin erstattete die Heimleiterin eine Vermisstenanzeige bei der Polizei. Auf Nachfrage im Klinikum erhielt die Polizei die Auskunft, dass sich der Patient auf der Diabetes-Station befinde.

Nach Art. 5 Abs. 1 Buchstabe d) DS-GVO müssen personenbezogene Daten „sachlich richtig und […] auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)“. Zudem müssen personenbezogene Daten nach Art. 5 Abs. 1 Buchstabe f) DS-GVO „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)“. Der Verantwortliche ist für die Einhaltung dieser Vorgaben verantwortlich und muss deren Einhaltung nachweisen können („Rechenschaftspflicht“), Art. 5 Abs. 2 DS-GVO.

Ganz offensichtlich waren die personenbezogenen Daten des Patienten im vorliegenden Fall jedoch nicht richtig und wurden durch das Klinikum auch nicht berichtigt. Daher nahm der TLfDI den eingangs erwähnten Zeitungsartikel im Juli 2019 zum Anlass und wandte sich mit einem Auskunftsersuchen an das Klinikum, um den tatsächlichen Zustand beziehungsweise den Verbleib des Patienten zu erfahren.

Hierbei stellte sich heraus, dass der Patient zu den Zeitpunkten der vom Klinikum erteilten Auskünfte bereits verstorben und in die Pathologie gebracht worden war. Der TLfDI stellte fest, dass das KIS zur Verwaltung von Patienten- und medizinischen Daten korrekt funktionierte und die fehlerhaften Auskünfte des Klinikums zum Verbleib des Patienten insofern nicht auf falschen Informationen der technischen Systeme beruhten.

Für die Auskunftserteilung gegenüber Angehörigen von Patienten des Klinikums steht den Klinikmitarbeitern eine sogenannte digitale „Pförtnerliste“ zur Verfügung. Wird die Liste über den Namenseintrag und das Geburtsdatum des nachgefragten Patienten aufgerufen, so werden die Station, das Zimmer und der Vitalzustand des Patienten angezeigt. Im vorliegenden Fall war für den Patienten in der Pförtnerliste richtig vermerkt „am 24. Mai 2019 verstorben“. Dennoch erteil-

ten verschiedene Klinikmitarbeiter zu verschiedenen späteren Zeitpunkten die Auskunft, dass sich der Patient auf der kardiologischen Station im Klinikum befinde. Hieraus ergab sich die Vermutung, dass der Patient in der Pathologie vom Personal des Klinikums schlicht „vergessen“ wurde. Im Hinblick auf die Mitteilung des Klinikums gegenüber der Polizei legte das Klinikum dar, dass es sich bei der Information, dass der Patient auf der Diabetesstation liege, um eine namentliche Patientenverwechslung handelte, da ein Patient mit gleichem Namen zu dieser Zeit im Klinikum behandelt wurde.
Durch den Vorfall wurde deutlich, dass das Klinikum nicht über ausreichende technische und organisatorische Maßnahmen nach Art. 32 DS-GVO verfügt, um die Integrität von Patientendaten zu schützen. Dies bezieht sich insbesondere auf Daten von Patienten, die keine Angehörigen haben, sondern einen gesetzlichen Betreuer beziehungsweise Patienten, die aus einem Seniorenheim ins Klinikum eingeliefert werden. Auf Nachfrage des TLfDI teilte die Datenschutzbeauftragte des Klinikums mit, dass es keine allgemeine Richtlinie oder Dienstanweisung im Klinikum gibt, wie in solchen Fällen zu verfahren ist, das heißt, an wen welche Informationen weitergegeben werden. Der TLfDI hielt eine solche Richtlinie aus Datenschutzgründen jedoch für zwingend erforderlich, um derartige Vorfälle in Zukunft zu vermeiden und für alle Klinikmitarbeiter eindeutige Handlungsvorgaben festzulegen. Zudem ist aufgrund der Altersstruktur unserer Gesellschaft davon auszugehen, dass derartige Fälle häufiger vorkommen können. Daher forderte der TLfDI das Klinikum auf, eine entsprechende Richtlinie gemäß den Vorgaben von Art. 32 Abs. 1 DS-GVO zu erstellen und dem TLfDI zu übersenden. Dies erfolgte schließlich im Mai 2020.

4.11 Datenschutz im Krankenhaus: Wenn der Expartner die Patientenakte „filzt“

Gesundheitsdaten unterliegen einem besonderen Schutz. Ein datenschutzkonformes Rollen- und Rechtekonzept für Zugriffe von Krankenhausmitarbeitern auf Patientenakten muss technisch so gestaltet sein, dass jeder Mitarbeiter nur über Zugriffsrechte für seinen medizinischen Anwenderbereich (beispielsweise „Pflege“) in seinem eigenen klinischen Fachbereich beziehungsweise auf seiner Station verfügt.

Mitte September 2020 meldete ein Thüringer Klinikum dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Datenpanne, bei der ein Klinikmitarbeiter unbefugt Einsicht in die elektronisch gespeicherte Patientenakte seiner ehemaligen Lebensgefährtin und deren neugeborenem Kind genommen hat. Als Begründung hatte der Klinikmitarbeiter angegeben, dass es sich beim Kind seiner ehemaligen Lebensgefährtin um sein Kind handele. Die datenschutzrechtliche Prüfung der Angelegenheit auf Grundlage von Art. 58 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) durch den TLfDI ergab, dass der Klinikmitarbeiter, der im Fachbereich „Psychiatrie/ Psychotherapie“ des Klinikums tätig war, auch über Zugriffsrechte auf Patientenakten des Fachbereichs „Frauenheilkunde und Geburtshilfe“ verfügte. Aus der vom TLfDI hierzu geforderten Stellungnahme des Klinikums ging hervor, dass offensichtlich alle Mitarbeiter des Klinikums nicht nur Zugriffsrechte auf Patientendaten ihrer eigenen Arbeitsbereiche, sondern auch auf Patientendaten anderer Stationen des Klinikums besaßen.
Für Zugriffe auf Patientenakten muss datenschutzrechtlich sichergestellt sein, dass nur befugte Personen (behandelnde Ärzte, Schwestern, Pfleger) Zugriff auf die Akten haben, das heißt jeder Mitarbeiter nur Zugriffsrechte auf Patientenakten „seines“ klinischen Fachbereichs beziehungsweise „seiner“ Station besitzt. Falls ein patientenbezogener erweiterter Zugriff (beispielsweise ein erweiterter Anwender- oder Stationsbereich) von Mitarbeitern erforderlich sein sollte, müssen entsprechende erweiterte Rechte punktuell und nachvollziehbar durch die IT im elektronischen Krankenhausinformationssystem (KIS) vergeben werden. Diese Vorgehensweise wurde jedoch im Klinikum nicht praktiziert. Somit war das Rollen- und Rechtekonzept des KIS für Zugriffe auf Patientenkaten nicht datenschutzkonform im Sinne von Art. 32 DS-GVO, das heißt, die geforderten organisatorischen und technischen Maßnahmen, um personenbezogene (Gesundheits-)Daten vor dem unbefugten Zugriff zu schützen, wurden nicht eingehalten.
Der TLfDI forderte vom Klinikum, das Rollen- und Rechtekonzept für Zugriffe von Klinikmitarbeitern auf Patientenakten umgehend datenschutzkonform einzurichten. Auf der Grundlage von Art. 58 Abs. 2 Buchstabe d) DS-GVO forderte der TLfDI das Klinikum auf, folgende Maßnahmen gemäß Art. 32 DS-GVO sofort umzusetzen:

- die Zugriffsbefugnisse der einzelnen Rollen sofort einzuschränken und Rollenwechsel in der IT-Abteilung des Klinikums prioritär zu bearbeiten,

- den elektronischen „Behandlungsauftrag für Notfälle“ in Betrieb zu nehmen, um abzusichern, dass jeder Zugriff auf Patientenakten, der außerhalb des jeweiligen Fachbereichs liegt, nicht ohne fachliche Begründung erfolgen kann und in den Logfiles (Protokolldateien über erfolgte Zugriffe) vermerkt wird. Durch diese „Überwachungsoption“ wird die psychologische Schranke für eine solchen Zugriff erhöht.

Das Klinikum erfüllte die Forderung und teilte dem TLfDI mit, dass zum 1. Dezember 2020 „…alle Zugriffe auf Patienten außerhalb des eigenen Zuständigkeitsbereiches uneingeschränkt protokolliert [werden].“ Außerdem werden die Mitarbeiter bei jedem Zugriff außerhalb des eigenen Zuständigkeitsbereiches durch einen schriftlichen Hinweis vor einem unberechtigten Zugriff gewarnt: *„Achtung! Zugriff darf nur erfolgen, wenn für Behandlung erforderlich!“*

Das Klinikum fragte beim TLfDI noch nach, durch welchen Geschäftsbereich des Klinikums missbräuchliche Zugriffe auf Patientenakten in welchen zeitlichen Abständen datenschutzkonform zu identifizieren sind und wie mit dem Verdacht missbräuchlicher Zugriffe umzugehen ist. Der TLfDI empfahl dem Klinikum, regelmäßig eine Stichprobe aus den Logfiles zu ziehen und den Zugriffsgrund zunächst beim Mitarbeiter persönlich zu erfragen. Nach Auffassung des TLfDI sollte hier eine Stichprobenziehung mit circa 20 Proben alle drei Monate genügen, um auch auf die abschreckende Wirkung der Prüfmaßnahmen zu setzen. Sobald auch die Protokollierung des Zugriffsgrundes technisch umgesetzt ist, können Menge und Häufigkeit der Stichproben so angepasst werden, dass der Stichprobenumfang einen vom Klinikum konkret festgelegten Prozentsatz der Belegschaft erfasst, um Missbrauchsfälle zu identifizieren.

Zur Frage, durch welches Klinikpersonal beziehungsweise welchen Geschäftsbereich missbräuchliche Zugriffe ausgewertet und erörtert werden sollten, wies der TLfDI das Klinikum darauf hin, dass der Zugriff auf die Logfiles immer im 4-Augen-Prinzip mit dem Personalrat/Betriebsrat zu erfolgen hat und sinnvollerweise auch in Anwesenheit des betrieblichen Datenschutzbeauftragten. Hierzu ist zudem ein Bericht zu erstellen. Die Angestellten müssen gemäß Art. 12 in Verbindung mit Art. 13 DS-GVO über das Vorgehen der gezielten Kontrolle beziehungsweise der Stichproben (sowie den Grund für dieses Vorgehen, beispielsweise tatsächliche und/oder Verdacht auf Missbrauchsfälle) und die damit verbundene Verarbeitung ihrer personenbezogenen Daten umfänglich informiert werden.

4.12 Datenschutz und Corona-Zeiten – Pseudonymisierung der Kontaktdaten

Apps, die der Kontaktnachverfolgung bei einer Infektion mit dem Corona-Virus dienen sollen, unterliegen auch den datenschutzrechtlichen Vorgaben der DS-GVO. So sind dem Stand der Technik entsprechende sichere Verschlüsselungsverfahren und Zugriffsberechtigungen bei der Datenerfassung, der Datenspeicherung und Datenübertragung vorzusehen.

Die Corona-Pandemie hat die Gesellschaft vor große Herausforderungen gestellt. So müssen Kontaktdaten von Bürgern bei Veranstaltungen, Sportereignissen, in der Gastronomie, im Gesundheitsbereich (Arztpraxen, Krankenhäuser), bei Vorlesungen und im Hotelgewerbe erfasst werden. Entsprechend den jeweils geltenden gesetzlichen Regelungen (https://corona.thueringen.de/) sind diese Kontaktdaten vier Wochen vom Veranstalter, Betreiber, Gastwirt, Arzt oder der Einrichtung aufzubewahren und anschließend zu vernichten. Da dies in der Praxis zu sehr viel Zettelwirtschaft und einer zusätzlichen Belastung der Verantwortlichen führte, etablierten sich Apps auf dem Markt für die unterschiedlichen Anwendungsfälle, welche die Erfassung der Kontaktdaten erleichtern sollen. Gerade ab Sommer 2020 erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zahlreiche Anfragen, inwieweit bestimmte Apps zur Kontaktdatenerfassung bei Vorlesungen, bei Veranstaltungen oder im Gastronomiegewerbe datenschutzrechtlich zulässig sind. Dabei gab es gute Ideen und weniger gute Ideen.
Weniger gut war eine Idee, die Klardaten einfach auf einem zentralen Server zu speichern und beim Kontaktformular einfach anstelle des Namens den Link zur Webseite und ein Passwort anzugeben. Die Kontaktdaten wurden auf dem Server niemals gelöscht und konnten vom Betreiber vollumfänglich eingesehen werden. Dieses Konzept entsprach aus diesen Gründen selbstverständlich nicht den rechtlichen Vorgaben, insbesondere dem Recht auf Löschung nach Art. 17 Datenschutz-Grundverordnung (DS-GVO).
Andere Konzepte basieren darauf, die Daten so zu verschlüsseln, dass entweder nur der Verantwortliche darauf zugreifen kann oder nur noch das Gesundheitsamt (und der Verantwortliche nicht mehr). Hier können Gäste ihre Kontaktdaten ohne Zutun des Gastwirtes/ Verantwortlichen auf einer Plattform registrieren – oft ist nur das Scannen eines

QR-Codes durch einen der Beteiligten notwendig – und auch das Löschen des Kontaktes nach der Speicherfrist erfolgt auf diesen Plattformen automatisch. Alle diese Lösungen haben die Gemeinsamkeit, dass die Kontaktdaten verschlüsselt auf dem Server des Betreibers gespeichert sind. Je nach Verschlüsselungskonzept müssen bei der Entschlüsselung mehrere unterschiedliche Teilnehmer (zum Beispiel Verantwortlicher und Gesundheitsamt) ihre Schlüssel kombinieren, um die Kontaktdaten wieder zu entschlüsseln. Diese Kombination erfolgt dann erst im Infektionsfall. Damit liegen die Daten auf den Servern in pseudonymisierter Form vor und sind teilweise für die Verantwortlichen sogar so lange nicht entschlüsselbar, wie keine gemeldete Infektion eines Betroffenen vorliegt. Auf dieser Basis hat der TLfDI den Einsatz einer App für Studierende in Vorlesungen und für Veranstalter für zulässig erachtet.
Eine andere App für die Gastronomie wird mit den entsprechenden Stellen zusammen gerade evaluiert. Insgesamt kann man für die als „gut“ befundenen Apps sagen, dass ihr Sicherheitsniveau über dem der Papiererfassung liegt und auch der Aufwand der Verantwortlichen für die Erfassung der Daten dabei sinkt.
Nicht verwechseln sollte man diese Apps mit der Corona-Warn-App des Bundes. Hier werden tatsächlich nur anonyme Kontaktdaten ausgetauscht, bei denen weder das Serversystem noch die empfangenden Smartphones einen Personenbezug zu den Kontakten wiederherstellen kann (siehe Beitrag 2.4).

4.13 Wenn das Krankenhaus sagt: „Eine Kopie gibt's nie!“ ...dann hilft der TLfDI

Gemäß Art. 15 Abs. 3 DS-GVO muss das Krankenhaus (beziehungsweise Klinikum oder der behandelnde Arzt) dem betroffenen Patienten auf Anforderung eine (kostenfreie) Kopie seiner personenbezogenen (Gesundheits-)Daten aushändigen. Stellt der/die betroffene Patient/in den Antrag auf eine Kopie seiner/ihrer verarbeiteten Daten elektronisch, so ist die Kopie in einem gängigen elektronischen Format zur Verfügung zu stellen (vergleiche Art. 15 Abs. 3 Satz 3 DS-GVO).

Im September 2020 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über ein Krankenhaus. Die Beschwerdeführerin hatte das Kranken-

haus im August 2020 gebeten, ihr gemäß Art. 15 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) eine Kopie der personenbezogenen Daten und Informationen ihrer Patientenakte zu übersenden. Das Krankenhaus übersandte die angeforderten Dokumente nicht, sondern die betriebliche Datenschutzbeauftragte teilte der Beschwerdeführerin mit, dass die von ihr angeforderten Patientendaten keine personenbezogenen Daten seien, da lediglich Name, Anschrift und Telefonnummer personenbezogene Daten seien. Die Beschwerdeführerin habe daher kein Recht, diese Daten anzufordern und auch noch kostenfrei zu erhalten.

Der TLfDI wies das Krankenhaus darauf hin, dass seine datenschutzrechtlich vertretene Auffassung völlig unzutreffend ist. Denn nach Art. 4 Nr. 1 DS-GVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind…“.

Gemäß Art. 15 Abs. 3 Satz 1 und Satz 2 DS-GVO stellt der Verantwortliche „…eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.“ Hieraus ergibt sich die Verpflichtung, die erste Kopie der verarbeiteten personenbezogenen Daten kostenfrei zur Verfügung zu stellen und nur für Folgekopien ein Entgelt zu erheben. Erwägungsgrund 63 Satz 2 DS-GVO präzisiert, dass sich dies auch auf personenbezogene Patientendaten bezieht: Das Auskunftsrecht „…schließt das Recht betroffener Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.“

Der TLfDI wies das Krankenhaus deutlich auf diese Rechtslage der DS-GVO hin und forderte das Krankenhaus auf, der Beschwerdeführerin umgehend die angeforderten Patientendaten zu übersenden und

zwar, da es eine Erst-Anfrage war, kostenfrei (siehe hierzu auch Entscheidung des Sozialgerichts Dresden (Urteil vom 29. Mai 2020 Az. 6 O 76/20). Dieser Aufforderung kam das Krankenhaus umgehend nach und übersandte der Beschwerdeführerin eine Kopie ihrer eigenen Patientenakte.

4.14 Beschwerde über eine Pflegeeinrichtung wegen Veröffentlichung des Arbeitsvertrages in einer WhatsApp-Gruppe

Eine Pflegeeinrichtung nutzt zur internen Kommunikation den Messenger-Dienst WhatsApp. Der betriebliche Einsatz von Kommunikationsdiensten wie WhatsApp gerade im Gesundheitswesen ist nahezu in allen Fällen datenschutzrechtlich unzulässig.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde, dass in einer Pflegeeinrichtung zur internen Kommunikation vom Geschäftsführer der Messenger-Dienst WhatsApp eingesetzt wurde. In der WhatsApp-Gruppe wurde vom Geschäftsführer versehentlich die erste Seite des Arbeitsvertrages eines dort beschäftigten Mitarbeiters veröffentlicht.
Dieser spezielle Einsatz von Messenger-Diensten wie WhatsApp wird auch in Pflegeinrichtungen immer beliebter. Sie verkennen dabei jedoch zumeist die datenschutzrechtliche Brisanz dieser Unternehmung. Bei der Veröffentlichung der personenbezogenen Daten des betroffenen Beschäftigten aus der ersten Seite des Arbeitsvertrages handelt es sich um besonders schutzbedürftige personenbezogene Daten eines Beschäftigten. Die Weitergabe von personenbezogenen Beschäftigungsdaten an unternehmensinterne Stellen oder Dritte stellt eine rechtfertigungsbedürftige Datenverarbeitung nach Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) dar. Die dort genannte „Offenlegung von Daten“ bezeichnet jeden Vorgang, der dazu führt, dass die Daten an Dritte gelangt sind und somit zugänglich gemacht werden und diese sie auslesen oder abfragen können. Sie kann durch Datenübermittlung, Verbreitung oder Bereitstellung erfolgen. Einen solchen Verstoß sieht der TLfDI vorliegend in der Übermittlung aus der ersten Seite des Arbeitsvertrages durch den Geschäftsführer, die in die WhatsApp Gruppe des Unternehmens gestellt wurde, an alle Mitglieder dieser Gruppe.
Personenbezogene Daten von Beschäftigten dürfen nach § 26 Bundesdatenschutzgesetz nur für Zwecke des Beschäftigungsverhältnisses

verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenen Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Eine solche Erforderlichkeit für die Veröffentlichung der ersten Seite des Arbeitsvertrages ist in diesem Fall nicht gegeben. Der TLfDI verwies darauf, dass der betriebliche Einsatz von Kommunikationsdiensten wie WhatsApp auf privaten oder betrieblichen Endgeräten der Beschäftigten – gerade im Gesundheitswesen – in nahezu allen Fällen datenschutzrechtlich unzulässig ist. Gerade, weil bei der Nutzung von WhatsApp automatisch das lokal hinterlegte Adressbuch der Gruppen Mitglieder ausgelesen und alle diese Kontaktdaten ungefragt an WhatsApp übermittelt werden (siehe Beitrag 4.7).
Für den Umstand, dass der Verantwortliche ohne Vorliegen einer Rechtsgrundlage die erste Seite des Arbeitsvertrages in der unternehmensinternen WhatsApp-Gruppe veröffentlicht hat, wurde unter der Abwägung der Art und Weise des entstandenen Schadens von den zur Verfügung stehenden Abhilfemaßnahmen aus Art. 58 Abs. 2 DS-GVO das Mittel der Verwarnung gewählt.

4.15 Beschwerde über Fragebogen „betreutes Wohnen“

Pflegedienste händigen Fragebogen an Pflegebedürftige aus, in denen diese über ihr Leben erzählen können. Diese Praxis ist ein wesentlicher Bestandteil der fach-pflegerischen Versorgung und Betreuung von Menschen mit Demenz. Aufgrund der fachlichen Notwendigkeit ist diese Datenerhebung unter Einhaltung bestimmter Voraussetzungen zulässig.

Eine Beschwerde richtete sich gegen den Betreiber einer Pflegeeinrichtung, da diese Pflegebedürftigen beziehungsweise deren Angehörigen einen Fragenbogen „Erinnerung an mein Erwachsenenalter“ zum Ausfüllen vorlegten. Die Angehörige hielt einige der dort aufgeführten Fragen für sehr persönlich und es war für sie nicht ersichtlich, was mit den erhobenen Daten geschehen soll. Mithilfe dieses Fragebogens werden sehr weitreichende biografische Daten und, im Hin-

blick auf Verwandtschaftsverhältnisse, teilweise auch Daten von Dritten erhoben.
Nach eingehender Stellungnahme des Betreibers der Pflegeeinrichtung sei der Fragebogen „Erinnerung an mein Erwachsenenalter“ ein wesentlicher Bestandteil der fach-pflegerischen Versorgung und Betreuung von Menschen mit Demenz. Damit einhergehend ist die Durchführung der Biographiearbeit ein Bestandteil der regelmäßigen Qualitätsprüfungen nach § 114 Sozialgesetzbuch XI des Medizinischen Dienstes der Krankenkassen. Der Fragebogen soll dabei helfen, die „untergehende, schwindende“ Identität von Pflegebedürftigen länger zu bewahren, weshalb es für den Pflegedienst wichtig ist, Daten aus der Vergangenheit, Gegenwart und Zukunft der Pflegebedürftigen zu erheben. Dies sind wichtige Informationen, um einen qualifizierten Umgang mit dem Krankheitsbild zu ermöglichen und einen angemessenen Kontakt zum Pflegebedürftigen wahren zu können.
Das Ausfüllen des Fragebogens sei freiwillig. Die Daten werden gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO) aufgrund einer Einwilligung des Pflegebedürftigen erhoben. Genutzt werde in diesem Zusammenhang ein standardisierter Fragebogen, welcher in der Pflegedokumentationsmappe des jeweiligen Pflegebedürftigen abgelegt werde. Lediglich die verantwortlichen Pflegekräfte hätten Zugriff auf die Angaben. Die zugriffsberechtigten Mitarbeiter würden schließlich auf das Dienstgeheimnis verpflichtet.
In der Einwilligungserklärung zur Biografiearbeit wurde nicht hinreichend über den Zweck der Erhebung, Verarbeitung und Nutzung der erhobenen Daten hingewiesen. Der Pflegeeinrichtung wurde mitgeteilt, dass eine Einwilligung nur wirksam ist, wenn sie freiwillig und konkret informiert ist. Daraufhin wurde von der Pflegeeinrichtung ein Muster vorgelegt, die den datenschutzrechtlichen Vorgaben entsprach.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit wies darauf hin, dass gerade bei demenzkranken Personen die biografischen Daten oft von dritten Personen wie Angehörigen oder Betreuungspersonen abgefragt werden. In diesem Fall ist zu beachten, dass die Pflegeeinrichtung dadurch, dass sie personenbezogene Daten nicht bei der betroffenen Person direkt, sondern bei Dritten erhebt, bestimmte Informationspflichten gegenüber der betroffenen Person hat (Art. 14 DS-GVO).
Kann ein Pflegebedürftiger aufgrund seiner Erkrankung nicht mehr selbst einwilligen, dann muss entsprechend der Gesetzeslage zum Bei-

spiel durch ein vom Betreuungsgericht bestellter Betreuer oder durch eine Versorgungsvollmacht benannte Person einwilligen.

4.16 Beschwerde gegen Vermieter wegen der unberechtigten Weitergabe einer Telefonnummer an den Handwerker

Der Vermieter darf die Telefonnummer des Mieters nicht ohne dessen Einwilligung an ein Handwerksunternehmen weitergeben.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen einer Beschwerde bekannt, dass eine Thüringer Wohnungsgesellschaft personenbezogene Daten verarbeitete, ohne hierfür berechtigt zu sein. Die Wohnungsgesellschaft hat im Rahmen von Baumaßnahmen an einem ihrer Häuser einem Handwerksunternehmen, das mit Bauleistungen beauftragt war, eine Liste mit den Namen und privaten Telefonnummern von Mietern zur Verfügung gestellt, damit diese zur Terminorganisation und Durchführung von Bauarbeiten kontaktiert werden konnten.
Dagegen wandte sich ein Mieter und erhob eine Beschwerde beim TLfDI wegen der unberechtigten Weitergabe seiner Telefonnummer an Dritte. Der TLfDI wandte sich sodann an die Wohnungsgesellschaft und wies auf die Rechtslage hin. Die Weitergabe der personenbezogenen Daten des Mieters durch Übermittlung seiner Telefonnummer an das Handwerksunternehmen stellt einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) dar. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Diese Fälle der rechtmäßigen Datenverarbeitung sind abschließend in Art. 6 Abs. 1 DS-GVO geregelt. Art. 5 Abs. 1 Buchstabe a) DS-GVO schafft folglich ein so genanntes Verbot mit Erlaubnisvorbehalt.
Eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO durch den Mieter lag nicht vor. Das vorgelegte Formular einer angeblich erteilten Einwilligungserklärung, welche alle Mieter unterzeichnen würden, genügte nicht den Anforderungen an eine Einwilligung. Diese Erklärung war nicht ausreichend bestimmt im Sinne des Art. 7 DS-GVO. Sie enthielt keinerlei Konkretisierungen durch Ankreuzen der von der Einwilligung abzudeckenden Sachverhalte. Die Einwilligungserklärung hatte daher keinen konkreten Erklärungsgehalt und war daher so zu werten, als ob sie nicht abgegeben wurde.

Als weitere Rechtsgrundlage für die Übermittlung der Telefonnummer an das Handwerksunternehmen kam auch nicht Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO in Frage. Nach dem Mietvertrag ist der Vermieter verpflichtet, den Mietgegenstand in vertragsgemäßem Zustand zur Verfügung zu stellen. Selbst wenn man Instandhaltungs- und Sanierungsmaßnahmen als Bestandteil der Vertragspflicht ansieht, ist die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO für die Übermittlung der Telefonnummer an Dritte hier nicht einschlägig. Aufgrund des Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist die Verarbeitung im Rahmen der Erfüllung des Vertragsverhältnisses möglich. Die Weitergabe der Telefonnummer an Dritte diente jedoch nicht der Erfüllung des Vertragsverhältnisses mit dem Mieter. Selbst für den Fall, dass die Handwerksleistung im Rahmen der Vertragserfüllung läge, ist die Datenübermittlung dazu nicht erforderlich, da es mildere Mittel gibt. Hier ist es nur möglich, dass die Telefonnummer durch die Wohnungsgesellschaft selbst genutzt wird, um Anrufe beim Mieter für kurzfristige Absprachen zu tätigen.
Schlussendlich wurde als weitere Rechtsgrundlage der Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO geprüft. Die Befugnis zur Übermittlung der Telefonnummer kann jedoch auch nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden. Eine Verarbeitung personenbezogener Daten ist danach rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dafür müsste die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich gewesen sein. Wenn die berechtigten Interessen auf anderem Wege ebenso effektiv verwirklicht werden können und hierbei die Rechte und Interessen der betroffenen Person weniger beeinträchtigt werden, ist eine Verarbeitung schon nicht erforderlich. Dies zu Grunde gelegt, war es daher nicht erforderlich, den direkten Kommunikationsweg zur Terminabsprache zwischen den Mietern und der Handwerksfirma zu ermöglichen, da auch eine Information an den Mieter durch die Wohnungsgesellschaft selbst hätte erfolgen können, ohne die Übermittlung der Telefondaten an einen Dritten. Es gab daher keine rechtliche Grundlage zur Übermittlung der Telefonnummerndaten des Mieters an das Handwerksunternehmen und es liegt daher eine rechtswidrige Verarbeitung der Daten vor.

Der TLfDI erließ daraufhin eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO, um zukünftig ein datenschutzkonformes Verhalten der Wohnungsgesellschaft bei ähnlichen Fällen herbeizuführen und Verstöße in der Zukunft zu unterbinden.

4.17 Datenerfassung bei Wohnungsbaugenossenschaft und Bonitätsauskunft bei Wohnungsanfragen

Die umfangreiche Datenerhebung in einem Anmeldeformular und die Implementierung einer standardmäßigen Bonitätsabfrage durch den Vermieter zu einem Zeitpunkt, an dem der Abschluss eines Mietvertrages noch nicht einmal im Raum steht, ist mit den Grundsätzen der Datenverarbeitung nach Art. 5 DS-GVO und auch des Art. 6 Abs. 1 Satz 1 Buchstaben b) und f) DS-GVO nicht vereinbar.

Aufgrund einer Beschwerde wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass bei einer Thüringer Wohnungsbaugenossenschaft bei einer bloßen Interessenbekundung eines Wohnungsinteressenten und seiner Nachfrage dahingehend, ob überhaupt freie Wohnungen in einem bestimmten Gebäudekomplex vorhanden sind, ein umfangreicher Wohnungsantrag und damit verbunden eine Einverständniserklärung zur Übermittlung von Daten an eine Auskunftei zum Zwecke der Kreditwürdigkeitsprüfung abgegeben werden muss.
Der Beschwerdeführer kam dieser Forderung zunächst nach, da er an einer Wohnung interessiert war, widerrief dann aber noch während des Gespräches seine Einwilligung und nahm auch seinen Wohnungsantrag zurück. Dabei wurde ihm allerdings mitgeteilt, dass bereits alle notwendigen Daten für die Kreditwürdigkeitsüberprüfung an die Auskunftei übermittelt worden seien. Daraufhin fragte der Betroffene beim TLfDI nach, ob ein derartiges Verfahren zulässig sei und beschwerte sich über die Wohnungsbaugenossenschaft. Der TLfDI forderte sodann die Wohnungsbaugenossenschaft auf, den Sachverhalt zu erklären und zu diesem Verfahren Stellung zu nehmen. Der TLfDI ließ sich auch das Antragsformular zur Prüfung übersenden.
Nach Prüfung der Angaben zum Verfahrensablauf bei Anfragen oder Interessenbekundungen zum Anmieten einer Wohnung wurde festgestellt, dass dieses Verfahren nicht den Vorgaben der Datenschutz-Grundverordnung (DS-GVO) entspricht und auch den von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und

der Länder (DSK) verabschiedeten Hinweise in der „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten“ (OH Mietinteressenten) vom 30. Januar 2018 und dem darin niedergelegten rechtmäßigen Umgang mit Daten von Mietinteressenten und zukünftigen Mietern nicht entsprochen wurde.
Die Wohnungsbaugenossenschaft war der Ansicht, dass der Antrag vollständig auszufüllen ist und ohne die Abfrage zur Bonität die Anfrage nicht bearbeitet werden kann und stützte sich dabei auf Art. 6 Abs. 1 Satz 1 Buchstaben b) und f) DS-GVO sowie auf genossenschaftliche Grundsätze zur Abwendung von Schaden für die Genossenschaft.
Gemäß Art. 5 Abs. 1 der DS-GVO müssen Daten auf rechtmäßige Weise verarbeitet werden. Wann eine solche Verarbeitung rechtmäßig ist, ergibt sich indes aus Art. 6 DS-GVO. Die Verarbeitung ist danach nur dann rechtmäßig, wenn eine der dort genannten Rechtsgrundlagen für die Verarbeitung herangezogen werden kann. Im Falle der Wohnungsbaugenossenschaft war kein Fall des Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO gegeben, da es zwar um eine vorvertragliche Maßnahme ging, es aber an der Notwendigkeit der Datenerhebung für den entsprechenden Zweck mangelte. Die OH Mietinteressenten der DSK legt für verschiedene Stadien im Rahmen der Wohnungsanmietung verschiedene Datenkategorien fest, die erhoben werden dürfen, weil ihre Kenntnis in diesem Stadium erforderlich ist. Bei bloßem Interesse an der Anmietung einer Wohnung und einer damit verbundenen Besichtigung besteht allein die Notwendigkeit dafür, dass die Adressdaten des Interessenten aufgenommen werden dürfen. Gegebenenfalls darf nach dem Vorliegen eines Wohnberechtigungsscheines gefragt werden, sofern die Wohnung nur damit vermietbar ist.
Im Rahmen einer unverbindlichen Voranfrage, ob es überhaupt in einem bestimmten Gebiet gerade verfügbaren Wohnraum gibt, ist die Notwendigkeit irgendeiner Datenerhebung indes fraglich. Warum hier ein Antrag auszufüllen war, ist nicht nachvollziehbar und diese Vorgehensweise entspricht auch nicht dem Grundsatz der Datensparsamkeit nach der DS-GVO. Aus diesem Grund kam der TLfDI zu dem Ergebnis, dass hier die Datenverarbeitung auch gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO nicht möglich ist, da es kein berechtigtes Interesse eines Vermieters darstellt, im Rahmen einer unverbindlichen Auskunft über die Verfügbarkeit von Wohnraum einen umfangreichen Anmeldbogen auszufüllen und eine Bonitätsabfrage zu tätigen.

Der Wohnungsantrag beinhaltete Datenerhebungen, die zum Zeitpunkt der Interessenbekundung in diesem Umfang nicht gerechtfertigt sind, sondern erst dann, wenn sich der Interessent für eine bestimmte Wohnung entscheidet und damit ein möglicher Vertragsabschluss überhaupt im Raum steht.
Neben diesen Daten beinhaltete der Antrag auch die Genehmigung zur Einholung der Bonitätsauskunft. Verweigerte der Interessent die Zustimmung zur Bonitätsabfrage bei der Antragstellung, wurde der Wohnungsantrag nicht bearbeitet. Aus diesem Sachverhalt folgt jedoch, dass die Einwilligung, die für die Bonitätsabfrage eingeholt wurde, nicht gemäß Art. 7 DS-GVO erfolgte. Es fehlt an der Freiwilligkeit der Einwilligungshandlung, wenn die betroffene Person im Stadium einer Auskunft über die Wohnungssituation keine Einwilligung zur Bonitätsabfrage erteilt und ihr dann dargelegt wird, dass keine Bearbeitung erfolgt, bis die Einwilligung erteilt wird. Dies stellt eine Zwangssituation dar, aus der keine gültige Einwilligung hervorgehen kann und in diesem Fall auch nicht hervorgegangen ist. Wenn die Erbringung einer Dienstleistung von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig gemacht wird, die für die Erfüllung der Dienstleistung nicht erforderlich sind, spricht man auch vom sogenannten Koppelungsverbot, Art. 7 Abs. 4 DS-GVO. Da die Abfrage bei der Auskunftei auch im Rahmen einer Anfrage zu der Verfügbarkeit von Wohnraum von keiner rechtlichen Grundlage gedeckt ist, stellt dies einen tiefgreifenden Eingriff in die Rechte und Freiheiten der betroffenen Person dar und ist in jedem Fall eine unzulässige Datenverarbeitung.
Auch der Vortrag, Schaden von der Genossenschaft abzuwenden, geht ins Leere, da der Nachweis über eine bestehende Bonität an späterer Stelle geführt werden kann für den Fall, dass dahingehend Bedenken bestehen. Erst bei Abschluss eines Mietvertrages, und auch nur dann, kann es zu einem Schaden führen, die Bonität des künftigen Mieters nicht zu kennen. Daher ist auch in der OH Mietinteressenten der DSK für den Fall des Abschlusses eines Mietvertrages die Möglichkeit vorgesehen, dass der Mietinteressent selbst zum Nachweis seiner Bonität für den speziellen Fall der Eingehung eines Mietverhältnisses entsprechende Auskünfte bei der Auskunftei zur Vorlage beim Vermieter abfordern kann. Eine komplette „Selbstauskunft“ kann jedoch nicht gefordert werden, da diese weit mehr Angaben enthält als notwendig sind. Liegen beim Vermieter in Folge dieses Verfahrens bereits ausreichende Informationen über die Bonität der Mietinteressenten vor,

ist eine vom Vermieter veranlasste zusätzliche Bonitätsauskunft in jedem Fall unzulässig, da es auch hier an der Notwendigkeit fehlt. An dieser fehlt es aber eben auch, wenn die Frage, ob der Interessent überhaupt Wohnraum anmieten möchte und ob ein solcher auch derzeit zur Verfügung steht, noch gar nicht beantwortet wurde.
Die Implementierung einer standardmäßigen Bonitätsabfrage durch den möglicherweise zukünftigen Vermieter zu einem Zeitpunkt, an dem der Abschluss eines Mietvertrages noch nicht einmal im Raum steht, ist mit den Grundsätzen der Datenverarbeitung nach Art. 5 DS-GVO und auch des Art. 6 Abs. 1 Satz 1 Buchstaben b) und f) DS-GVO nicht vereinbar.
Nach Prüfung des Sachverhaltes wurde die Wohnungsbaugenossenschaft vom TLfDI aufgefordert, die Datenerhebung entsprechend den Vorgaben der DS-GVO und der OH Mietinteressenten anzupassen und umzugestalten. Das Antragsformular wurde daher von der Wohnungsbaugenossenschaft neu gefasst und auch die Bonitätsabfrage wurde angepasst. Das Verfahren ist im Berichtszeitraum noch nicht vollständig abgeschlossen und dauert noch an, da eine abschließende Bewertung hinsichtlich der erfolgreichen Umgestaltung aller festgestellten Mängel durch den TLfDI noch aussteht.

4.18 Vorlage des Personalausweises bei Immobilienkauf erst bei ernsthafter Kaufabsicht erforderlich

Im Rahmen eines Immobilienkaufs kann die Vorlage des Personalausweises oder die Übermittlung seiner Kopie von einem Kaufinteressenten nur verlangt werden, wenn der Kaufinteressent seine Kaufabsicht bekundet hat. Diese kann bei der Vereinbarung eines Besichtigungstermins ohne weitere Hinweise auf die Kaufabsicht nicht angenommen werden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Bürgers, wonach er im Rahmen eines Immobilienkaufs für die Vereinbarung eines Besichtigungstermins dem Immobilienmakler eine Kopie seines Personalausweises übermitteln sollte. Der Kaufinteressent und Beschwerdeführer hatte sich augenscheinlich noch nicht zum Kauf der Immobilie entschlossen. Dennoch wurde die Kopie seines Personalausweises verlangt. Der Beschwerdeführer weigerte sich, dem nachzukommen und beschwerte sich beim TLfDI.

Grundsätzlich regelt § 20 Abs. 2 Personalausweisgesetz (PAuswG) die Zulässigkeit einer Anfertigung einer Personalausweiskopie. Nach § 20 Abs. 2 PAuswG darf der Personalausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig als Kopie erkennbar ist. Voraussetzung ist danach zunächst die Einwilligung des Ausweisinhabers zur Ablichtung, dies umfasst auch die Erstellung einer Fotokopie sowie die Erkennbarkeit dieser als Kopie (zum Beispiel als Schwarz-Weißdruck). Zudem wird eine datenschutzrechtliche Rechtfertigung entsprechend Art. 5 Abs. 1 Buchstabe a), Art. 6 Datenschutz-Grundverordnung (DS-GVO) verlangt. Als Rechtsgrundlage in Betracht kommt, neben der Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, die in diesem Fall gerade nicht vorlag, eine die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit einer weiteren Rechtsgrundlage (Art. 6 Abs. 3 DS-GVO).

Eine solche Verpflichtung ist für Personalausweiskopien in § 2 Nr. 14, § 8 Abs. 2, § 11 Abs. 2 und § 11a Geldwäschegesetz (GWG) normiert. Immobilienmakler sind nach § 2 Nr. 14 GWG Verpflichtete nach dem GWG. Entsprechend § 8 Abs. 2 GWG haben Verpflichtete das Recht und die Pflicht, Kopien von Dokumenten anzufertigen, die die Identität des Berechtigten anzeigen (mithin den Personalausweis). Nach § 11 Abs. 2 GWG dürfen Verpflichtete den Berechtigten allerdings nur dann identifizieren (und dies mittels Personalausweiskopie speichern), „wenn der Vertragspartner des Maklers ein ernsthaftes Interesse an der Durchführung des Immobilienkaufvertrages äußert“ (Kaufabsicht).

Das GWG stellt eine geeignete Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 Buchstabe c) und Abs. 3 DS-GVO dar. Danach müssen die Regelungen über die Datenverarbeitungen so klar und präzise die Verarbeitungsvoraussetzungen beschreiben, dass die Verarbeitungen für die Rechtsunterworfenen klar erkennbar ist (Kühling/ Buchner, Kommentar Datenschutzgrundverordnung, Art. 6 Rn. 84). Auch muss gemäß Art 6 Abs. 3 Satz 2 DS-GVO der Zweck der Verarbeitung gesetzlich festgelegt sein. § 11a GWG genügt diesen Anforderungen.

Mithin dürfen Immobilienmakler auf Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe c) und Abs. 3 DS-GVO in Verbindung mit § 2 Nr. 14, § 8 Abs. 2, § 11 Abs. 2 und § 11a GWG nur dann eine Kopie

des Personalausweises anfertigen, wenn eine Kaufabsicht der Immobilie seitens des Berechtigten vorliegt.
Zusätzlich muss die Datenverarbeitung entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO erforderlich sein. Art. 5 Abs. 1 Buchstabe c) DS-GVO statuiert das Prinzip der Datenminimierung, wonach Datenverarbeitungen auf das notwendige Maß beschränkt sein müssen. Das ist sie nur, soweit eine ernsthafte Kaufabsicht vorliegt.
Dem Verantwortlichen wurde mitgeteilt, dass das Verlangen des Personalausweises eines Kaufinteressenten ohne Kaufabsicht lediglich nach Einholung einer Einwilligung entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe a) und Art. 7 DS-GVO zulässig sei. Die bisher angewandte Praxis (Verlangen eines Personalausweises ohne Vorliegen einer Einwilligung und ohne Vorliegen einer Kaufabsicht) entsprach nicht den Vorgaben der DS-GVO. Dem Verantwortlichen wurde aufgegeben, seine Praxis umzustellen. Der Fall ist noch nicht abgeschlossen.

4.19 Übermittlung Mieterdaten an Grundversorger

Der Grundversorger kann vom Vermieter nicht verlangen, dass sofort bei Einzug die Mieterkontaktdaten an den Grundversorger übermittelt werden. Eine direkte anlasslose Meldepflicht seitens des Vermieters besteht nicht. Allenfalls nach Ablauf von sechs Wochen kann der Vermieter die Kontaktdaten des bisher nicht bei einem Stromversorger angemeldeten Mieters dem Grundversorger übermitteln.

Ein Vermieter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, er sei seitens seines Grundversorgers aufgefordert worden, sofort bei Einzug eines neuen Mieters die Kontaktdaten des Mieters an den Grundversorger zu übermitteln. Der Bürger bat um Mitteilung, ob dies datenschutzkonform sei. Der TLfDI konnte dem Bürger Folgendes darlegen:
Die Übermittlung von Mieterdaten an den Stromversorger stellt eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) dar. Der Vermieter wird zunächst gerade nicht Vertragspartner des Grundversorgers, da ja nicht er, sondern der Neumieter Vertragspartner werden soll. Daher kann Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO nicht als Rechtsgrundlage herangezogen werden. Die Rechtsgrundlage Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO bedarf entsprechend Art. 6 Abs. 3 DS-GVO

hierfür einer weiteren Rechtsgrundlage. Eine solche ist vorliegend nicht gegeben.
In Betracht kommt hier allenfalls eine zulässige Datenverarbeitung entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Danach ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Zunächst gilt, dass nach § 2 Abs. 2 der Verordnung über Allgemeine Bedingungen für die Grundversorgung von Haushaltskunden und die Ersatzversorgung mit Elektrizität aus dem Niederspannungsnetz (Stromgrundversorgungsverordnung – StromGVV) ein Vertrag mit dem noch unbekannten Mieter zu Stande kommt, sobald dieser Strom nutzt, ohne sich bei einem anderen Versorger anzumelden. In diesem Fall gilt eine Meldepflicht des Mieters gegenüber dem Grundversorger.
Soweit sich der Mieter nicht innerhalb von fünf Wochen und sechs Tagen bei einem Stromversorger angemeldet hat, wird, entsprechend der Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE, abrufbar unter: https://www.bundesnetzagentur.de/DE/Service-Funktio-nen/Beschlusskammern/BK06/BK6_83_Zug_Mess/831_gpke/20200527_Anlage1_GPKE.pdf?__blob=publicationFile&v=3) der Bundesnetzagentur, der Eigentümer/ Vermieter, selbst zur Grundversorgung angemeldet, da der Mieter dem Grundversorger noch unbekannt ist. Diese Frist beginnt mit der ersten Stromentnahme durch den neuen Mieter. Mithin trägt der Vermieter nach Ablauf dieser Zeit das Kostenrisiko für den verbrauchten Strom.
Zunächst muss jedoch die Anmeldung des eigentlichen Vertragspartners, sprich des Mieters, abgewartet werden. Zwar verringert die direkte Mitteilung der Mieterdaten durch den Vermieter an den Grundversorger das Kostenrisiko des Vermieters. Jedoch überwiegen in diesem Zeitraum nicht die berechtigten Interessen des Vermieters die schutzwürdigen Interessen des betroffenen Mieters. Dieser hat zudem das Recht, sich aus mehreren Stromanbietern für einen zu entscheiden. Durch direkte Anmeldung beim Grundversorger würde diese Wahlfreiheit konterkariert werden. Dabei entsteht das berechtigte Interesse des Vermieters nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO,

Mieterdaten an den Grundversorger zu übermitteln, erst mit Ablauf der fünf Wochen und sechs Tagen. Der Vermieter hat ein erhebliches Interesse daran, nicht das Kostenrisiko tragen zu müssen. Mithin überwiegen mit Ablauf dieser Frist seine berechtigten Interessen gegenüber dem schutzbedürftigen Interesse des Mieters. Der Vermieter darf nach Ablauf von sechs Wochen die Kontaktdaten an den Grundversorger melden.
Weiterhin wurde der Vermieter darauf hingewiesen, dass er die Daten auch auf Grundlage einer wirksamen datenschutzrechtlichen Einwilligung entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe a), Art. 7 DS-GVO übermitteln dürfe. Eine solche Einwilligung muss freiwillig, in informierter Weise und unmissverständlich erklärt werden, Art. 4 Buchstabe 11) DS-GVO. Wenn die Einwilligung durch eine schriftliche Erklärung erfolgt, muss das Ersuchen in verständlicher und leicht zugänglicher Form, in einer klaren Sprache und von anderen Sachverhalten klar zu unterscheiden sein, Art. 7 Abs. 2 DS-GVO. Die betroffene Person ist auch auf ihr Recht zum jederzeitigen Widerruf hinzuweisen. Ein bloßer Hinweis im Mietvertrag auf die etwaige Datenübermittlung an den Grundversorger reicht dazu jedoch nicht aus.

4.20 Authentifizierung kann zwar lästig sein – notwendig ist sie doch

Die DS-GVO stellt die Anforderung an Verantwortliche, dass sie geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Verarbeitung der personenbezogenen Daten systematisch zu schützen. Diese Maßnahmen schließen unter anderem die Fähigkeit ein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, so Art. 32 Abs. 1 Buchstabe b) DS-GVO.
Im Berichtszeitraum wandte sich ein Beschwerdeführer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, weshalb bei einem Telefonat mit einem Inkassounternehmen zusätzlich zur Kundennummer weitere Angaben wie das Geburtsdatum beim Authentifizierungsverfahren am Telefon abgefragt werden. Er trug vor, trotz einer Abfrage des bestehenden Aktenzeichens und einer Kundennummer keine Auskunft zu seinem Anliegen erhalten zu haben. Auch wurden ähnliche Vorgehensweisen bei einem Telekommunikationsanbieter und Krankenkasse vorgetragen.

Aufgrund des Beschwerdevortrags wies der TLfDI den Beschwerdeführer daraufhin, dass die Verantwortlichen gemäß Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) sicherzustellen haben, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit) ein. So müssen nach Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen bestimmt und umgesetzt werden, um die Verarbeitung von personenbezogenen Daten systematisch zu schützen und die Vertraulichkeit und die Integrität nach Art. 32 Abs. 1 Buchstabe b) DS-GVO sicherzustellen. Aus diesem Grund werden von den Verantwortlichen die Authentifizierungsverfahren durch die Abfrage zusätzlicher Angaben stärker abgesichert, um zu verhindern, dass Unberechtigte bei einer telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten. Die Vorgehensweise sah der TLfDI als datenschutzkonform an.

4.21 Wie löscht man sein Profil wieder von einem Portal?

Wenn die Rechtsgrundlage für die Registrierung in einem Forum die Einwilligung der betroffenen Person ist, kann sie ihre Einwilligung nach Art. 7 Abs. 3 DS-GVO widerrufen und die Löschung ihrer personenbezogenen Daten gemäß Art. 17 Abs. 1 Buchstabe b) DS-GVO verlangen.

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Beschwerde ein hinsichtlich der Löschung eines Accounts in einem Forum. Dabei schilderte der Beschwerdeführer, dass der Verantwortliche der Aufforderung zur Löschung seines Accounts nicht nachgekommen ist. Der Beschwerdeführer trug weiterhin vor, dass sein Account für ihn selbst gesperrt wurde. Für Dritte blieb der Account jedoch weiterhin sichtbar und im Forum konnten die Beiträge unter den Benutzernamen des Betroffenen weiter eingesehen werden.
Grundsätzlich gibt Art. 17 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) den betroffenen Personen ein Recht auf Löschung ihrer personenbezogenen Daten. Der Verantwortliche ist im Gegenzug verpflichtet, personenbezogene Daten unverzüglich zu löschen, wenn für

deren Speicherung keine Rechtsgrundlage bestand oder diese Rechtsgrundlage nicht mehr besteht. Die Rechtsgrundlage besteht etwa dann nicht mehr, wenn eine Einwilligung in die Verarbeitung und Nutzung der personenbezogenen Daten widerrufen wurde, so Art. 17 Abs. 1 Buchstabe b) DS-GVO. Allerdings besteht dieses Recht auf Löschung unter anderem dann nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.
So wandte sich der TLfDI an den Verantwortlichen des Forums und forderte ihn auf, personenbezogene Daten des Beschwerdeführers zu löschen. Der Verantwortliche handelte entsprechend der Aufforderung und löschte personenbezogene Daten des Beschwerdeführers, sodass das Benutzerprofil ferner nicht mehr abrufbar war.

4.22 Beschwerde über Nutzung von verlinkten Bildern bei Google

Im Rahmen seiner Beratungstätigkeit wurde der TLfDI angefragt, wie mit der Löschung von falsch verlinkten Bilden auf einem der Google-Dienste verfahren werden soll. Dem Betroffenen wurden Hinweise zu einer möglichen Vorgehensweise erläutert.

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und trug vor, dass er als Inhaber eines Handwerksbetriebes eine Visitenkarte auf Google MyBusiness habe. Dabei schilderte der Betroffene, dass auf der Visitenkarte Bilder von Kunden angezeigt werden, die keinen Bezug zu seiner Firma haben. Der Beschwerdeführer gab weiterhin an, dass er seit geraumer Zeit versuchte, die fremden Bilder zu entfernen und bat um Hinweise.
Zunächst war zu erläutern, dass Google mit MyBusiness einen Dienst für Unternehmen anbietet, damit diese ein Profil ihres Unternehmens erstellen können, welches angezeigt wird, falls ein Nutzer mit einer Google-Suche nach dem Unternehmen sucht. Bestandteile eines solchen Profils können Angaben zu Öffnungs- und Geschäftszeiten, Postadresse, Telefonnummer, Kategorie des Unternehmens und die Webseite sein. Darüber hinaus können auf der virtuellen Visitenkarte Bilder veröffentlicht werden, Dienstleistungen gebucht und Rezensionen hinterlassen werden. Ein anderer Dienst von Google ist Google Maps, ein Kartendienst. Dieser bietet eine Funktion, die es Nutzern erlaubt, Fotos an Google zu übermitteln und innerhalb von Google

Maps standortbezogen darzustellen. Dazu wertet Google die Standortinformationen des Fotos aus oder der Nutzer kann vor der Übermittlung an Google den Standort innerhalb von Google Maps festlegen. Auch werden innerhalb von Google Maps Unternehmen angezeigt und ein Nutzer kann eigene Bilder zuordnen und an Google übermitteln.
Dem Betroffenen wurde mitgeteilt, dass bei der Anzeige des Unternehmensprofils in der Google Suche nicht nur die Bilder angezeigt werden, die der Unternehmer in seinen MyBusiness Account hinterlegt hat, sondern auch die Bilder, die Nutzer in Google Maps mit dem Standort des Unternehmens verknüpft haben. Um die somit falsch zugeordneten Bilder zu löschen, wurde der Betroffene auf die Anleitung der Google MyBusiness und Google Maps zur Entfernung von Kundenfotos hingewiesen. Nähere Informationen finden sich unter: https://support.google.com/business/answer/6130451?co=GENIE.Platform%3DDesktop&hl=de&oco=0.

4.23 Beschwerde über eine Webseite wegen fehlender Datenschutzhinweise im Kontaktformular

Webseitenbetreiber bieten zur Kontaktaufnahme oft ein Kontaktformular an. Aus datenschutzrechtlicher Sicht sind dabei eine Transportverschlüsselung nach dem Stand der Technik erforderlich, wenn personenbezogene Daten abgefragt werden und der Grundsatz der Datensparsamkeit zu beachten ist.

Kontaktformulare, die auf Webseiten eingesetzt werden, ermöglichen es, die zur Bearbeitung einer Anfrage erforderlichen Informationen strukturiert zu erfassen. Auch bei Verwendung eines Kontaktformulars gilt der Grundsatz der Datensparsamkeit. Es dürfen nur die Daten erhoben werden, die auch tatsächlich für die Anfrage benötigt werden. Die Pflichtfelder im Kontaktformular müssen gekennzeichnet werden. Im Normalfall sind der Name und die E-Mail-Adresse oder die Telefonnummer für die Bearbeitung ausreichend.
Die im Kontaktformular erhobenen personenbezogenen Daten dürfen nur für den angegebenen Zweck verwendet werden. Nach der Zweckerfüllung müssen die Daten umgehend gelöscht werden und dürfen nicht für andere Zwecke verwendet werden. Der Verantwortliche der Webseite hat, wenn er über ein Kontaktformular personenbezogene Daten erhebt, nach Art. 32 Datenschutz-Grundverordnung (DS-GVO)

geeignete – dem Stand der Technik entsprechende – technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen.
Vielmals erfolgt die Datenübermittlung an den Verantwortlichen jedoch unverschlüsselt. Ist die Adresszeile mit einem „http“ versehen, zeigt dies, dass die Webseite nicht gesichert ist. Eine sichere Verbindung ist nur dann gewährleistet, wenn stets „https“ angezeigt wird. Ohne eine SSL-Verschlüsselung ist eine Webseite anfällig für Missbrauch der Daten Dritter. Werden vom Verantwortlichen keine Maßnahmen ergriffen, erfolgt eine unverschlüsselte Übermittlung. Die transportierten Inhalte können von allen Rechnern oder Netzwerkteilnehmern, die sich im gleichen Netzwerk befinden, mitgelesen oder verändert werden. In allen Fällen betrachtet der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine https-Verschlüsselung unabhängig vom Schutzbedarf als erforderlich. Bei einem normalen Schutzbedarf, also keine Übertragung von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO, sondern lediglich Name, Telefonnummer oder E-Mail-Adresse, ist eine Transportverschlüsselung mit „https“ notwendig und ausreichend. Werden im Kontaktformular besonders schutzbedürftige Daten nach Art. 9 DS-GVO abgefragt, ist zusätzlich zur https-Verschlüsselung auch eine Ende-zu-Ende-Verschlüsselung erforderlich.
Um dem Gebot der Transparenz zu entsprechen, ist es unerlässlich, dass das Kontaktformular einen Datenschutz-Hinweis mit den Informationen gemäß Art. 13 DS-GVO enthält. Dieser sollte so platziert werden, dass er für die Webseitenbesucher leicht zugänglich ist. Die Datenschutzerklärung muss sich auch auf das Kontaktformular beziehen. Sie muss die Angaben enthalten, welche Daten im Kontaktformular erhoben werden und die Zweckbindung für die einzelnen Angaben.
Aufgrund mehrerer Beschwerden hat der TLfDI festgestellt, dass immer noch unverschlüsselte Kontaktformulare auf Webseiten eingesetzt werden. Daraufhin wurden die Webseitenbetreiber auf die Mängel hingewiesen und es wurde auf eine datenschutzkonforme Verarbeitung hingewirkt.

4.24 Wenn der Arbeitgeber es gut meint, aber den Datenschutz außer Acht lässt

Beabsichtigt ein Arbeitgeber im Rahmen des betrieblichen Gesundheitsmanagements, eine betriebliche Zusatzkrankenversicherung zu-

gunsten seiner Beschäftigten anzubieten, sollte er vor der Weiterleitung der personenbezogenen Daten der Beschäftigten an eine private Krankenversicherungsgesellschaft unbedingt eine Einwilligung der Beschäftigten in diese Datenweiterleitung einholen. Hieran ändert auch nichts, dass der Arbeitgeber zuvor mit dem Betriebsrat eine Betriebsvereinbarung über das Anbieten einer solchen Zusatzversicherung getroffen hatte.

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) beschwerte sich eine Mitarbeiterin über das Verhalten ihres Arbeitgebers. Dieser hatte gemeinsam mit dem Betriebsrat eine Betriebsvereinbarung über die Einführung einer privaten Zusatzkrankenversicherung zugunsten der Beschäftigten getroffen. Die private Krankenversicherungsgesellschaft hatte der Arbeitgeber bereits ausgewählt und mit dieser als Versicherungsnehmer einen sogenannten Gruppenversicherungsvertrag abgeschlossen, in dem die Beschäftigten als versorgungsberechtigte Personen versichert werden sollten.

An sich eine gute Sache. Wenn der Arbeitgeber dabei nicht vorschnell personenbezogene Daten der Beschäftigten an die bereits ausgewählte Versicherungsgesellschaft weitergeleitet hätte, ohne die Beschäftigten vorab zu fragen, ob sie die angebotene Versicherung überhaupt möchten und sie mit einer Weitergabe ihrer Daten an die Krankenversicherung einverstanden sind. Der Arbeitgeber ging vielmehr davon aus, dass eine zuvor mit dem Betriebsrat geschlossene Betriebsvereinbarung über die Einrichtung und den Umfang der betrieblichen Krankenversicherung ausreichen würde, die Datenweiterleitung der Beschäftigtendaten zu rechtfertigen.

Dies sah der TLfDI anders. Die Betriebsvereinbarung enthielt eine Klausel, nach der der Beschäftigte zwar berechtigt war, der Datenweitergabe zu widersprechen. Dies reicht zum einen als Übermittlungsbefugnis nicht aus. Die Beschäftigten, die erst einen Tag vor der stattgefundenen Datenweitergabe über die beabsichtigte Einführung der betrieblichen Krankenzusatzversicherung informiert wurden, konnten zum anderen nicht verhindern, dass ihre Daten der Versicherung bekannt wurden.

Mit Beschäftigtendaten darf ein Arbeitgeber nicht leichtfertig umgehen. So ist eine Verarbeitung der personenbezogenen Daten der Beschäftigten grundsätzlich nur zulässig, wenn dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses

auch *erforderlich* ist. Dies ergibt sich aus Art. 88 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG). Doch was heißt *erforderlich*? Die Verarbeitung von personenbezogenen Daten von Beschäftigten muss geeignet und zugleich das relativ mildeste Mittel sein, um den unternehmerischen Interessen bei der Begründung, aber auch bei der Durchführung und Beendigung von Beschäftigungsverhältnissen Rechnung zu tragen (vergleiche Simitis, Hornung, Spiecker, Datenschutzrecht, DS-GVO mit BDSG, 1. Auflage 2019, Art. 88, Rn. 56 f.). Gemessen an diesen Maßstäben: Ist eine betriebliche Zusatzkrankenversicherung zugunsten der Beschäftigten erforderlich zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses? Klare Antwort: Nein.

Das Angebot mag von dem Arbeitgeber im zu entscheidenden Fall durchaus gut gemeint gewesen sein. Auch verkennt der TLfDI nicht, dass es im Einzelfall durchaus sinnvoll sein kann, eine zusätzliche private Absicherung im Krankheitsfall vorzuhalten. Aber dies führt vorliegend nicht zur Annahme einer *Erforderlichkeit* im Sinne des § 26 Abs. 1 Satz 1 BDSG. Schließlich kann das Beschäftigungsverhältnis auch ohne eine solche Zusatzversicherung fortgesetzt werden.

§ 26 Abs. 1 Satz 1 Halbsatz 2 BDSG sieht vor, dass personenbezogene Daten von Beschäftigten auch dann verarbeitet werden dürfen, wenn dies „zur Ausübung oder Erfüllung der sich […] aus einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist“. Dies betrifft zum einen den Unterrichtungsanspruch des Betriebsrates gegenüber dem Arbeitgeber nach § 80 Abs. 2 Satz 1 Betriebsverfassungsgesetz (BetrVG). Dabei sind dem Betriebsrat die zu seiner Aufgabenwahrnehmung (zum Beispiel aus §§ 99, 102, 112 BetrVG, aber auch aus Personalvertretungsgesetz der Länder und des Bundes oder dem Sprecherausschussgesetz) erforderlichen Informationen vom Arbeitgeber zur Verfügung zu stellen. Zum anderen sieht Art. 88 Abs. 1 DS-GVO in Verbindung mit § 26 Abs. 4 BDSG ausdrücklich vor, dass auch die Betriebsvereinbarung selbst tauglicher Erlaubnistatbestand für eine Datenverarbeitung sein kann (vergleiche Paal/ Pauly/ Gräber/ Nolden, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Beck’sche Kompakt-Kommentare, § 26 Rn. 19 f.). In einem solchen Fall bedarf es keines Rückgriffes auf § 26 Abs. 1 Satz 1 BDSG. Jedoch sind die Verhandlungspartner (also der Arbeitgeber und der Betriebsrat) dabei nicht von den strengen Vorgaben der

DS-GVO befreit, sondern müssen nach Art. 88 Abs. 2 DS-GVO selbst alle Maßnahmen zur Wahrung des Datenschutzniveaus der DS-GVO ergreifen. Eine Datenübermittlung an Dritte, wie hier an eine private Versicherungsgesellschaft, bedarf dabei stets einer (gesetzlichen) Rechtfertigung, die vorliegend nicht bestand. Die in der Betriebsvereinbarung enthaltene Widerspruchslösung wird dem nicht gerecht. Einzig mögliche Rechtfertigung war mithin eine ausdrückliche und vorab eingeholte Einwilligung der betroffenen Beschäftigten, die die Vorgaben des § 26 Abs. 2 BDSG erfüllt.
Eine solche Einwilligung der Beschäftigten wäre vorliegend nach § 26 Abs. 2 Satz 2 BDSG möglich und zulässig gewesen. Schließlich wollte der Arbeitgeber die Beiträge für die betriebliche Krankenversicherung ausschließlich und in vollem Umfang übernehmen, sodass den Beschäftigten ein finanzieller Vorteil entstünde.
Die Einholung einer Einwilligung von den Beschäftigten hat der Arbeitgeber im zu entscheidenden Fall jedoch unterlassen. Sich hierbei auf die Vereinbarung mit dem Betriebsrat und der darin enthaltenen Widerspruchslösung zu verlassen, war ein Trugschluss. Schließlich diente die Weiterleitung der Daten der Beschäftigten an die Versicherung auch nicht dazu, die Rechte und Pflichten des Betriebsrates aus der Betriebsvereinbarung zu erfüllen (§ 26 Abs. 1 Satz 1 BDSG), sondern vielmehr der Erfüllung der Arbeitgeberinteressen gegenüber der Krankenversicherung aus dem bereits abgeschlossenen Gruppenversicherungsvertrag. Der TLfDI stellte den Verstoß gegenüber der Verantwortlichen fest und sprach gemäß Art. 58 Abs. 2 Buchstabe b DS-GVO eine Verwarnung aus.

4.25 Erst AU-Bescheinigung – dann Kündigung: Ist das rechtens? Wie lange darf ein Arbeitgeber Arbeitsunfähigkeitsbescheinigungen der Beschäftigten aufbewahren?

Beim TLfDI ging die Anfrage eines Betriebsrates eines großen Unternehmens aus Thüringen ein, wie lange ein Arbeitgeber die krankheitsbedingten Fehltage der Beschäftigten speichern dürfe beziehungsweise, ob eine konkrete Speicherdauer von fünf Jahren zu lang bemessen sei. Der Arbeitgeber wollte diese Daten offensichtlich nutzen, um einzelnen Beschäftigten das Arbeitsverhältnis aus krankheitsbedingten Gründen zu kündigen.

Wie lange darf ein Arbeitgeber Daten über Krankschreibungen beziehungsweise krankheitsbedingten Fehltagen speichern? Wer in den Datenschutzgesetzen oder dem Entgeltfortzahlungsgesetz hierzu eine Regelung finden möchte, der sucht vergeblich. Die Antwort lautet wie so oft: Es kommt darauf an.

Datenschutzrechtlich greift zunächst der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 Buchstabe e) Datenschutz-Grundverordnung (DS-GVO). Danach dürfen personenbezogene Daten nur in einer Form gespeichert werden, „die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist". Oder einfacher ausgedrückt: Fällt der Zweck der Datenverarbeitung weg, so entfällt grundsätzlich auch die Berechtigung für eine weitere Datenverarbeitung in Form einer Speicherung der erhobenen Daten. Ausnahmen hierzu bilden gesetzliche Aufbewahrungsfristen.

Angewandt auf den konkreten Fall bedeutete dies: Grundsätzlich ist ein Arbeitgeber bei Ausspruch einer Kündigung gegenüber einem Beschäftigten für das Vorliegen der Kündigungsgründe darlegungs- und beweispflichtig. So auch bei einer krankheitsbedingten Kündigung. Eine Voraussetzung für eine wirksame krankheitsbedingte Kündigung ist eine sogenannte negative Gesundheitsprognose. Das heißt, der Arbeitgeber muss darlegen und beweisen können, wie lange ein Arbeitnehmer innerhalb eines gewissen Zeitraumes vor Ausspruch der Kündigung krankheitsbedingt gefehlt hat und es müssen zum Zeitpunkt der Kündigung Tatsachen vorliegen, die eine Prognose weiterer Erkrankungen wie im bisherigen Umfang erwarten lassen (§ 1 Abs. 2 Satz 4 Kündigungsschutzgesetz).

Zur Vorbereitung einer krankheitsbedingten Kündigung ist der Arbeitgeber dabei grundsätzlich gehalten, die angefallenen krankheitsbedingten Fehltage eines Beschäftigten aufführen zu können, was zwangsläufig eine Speicherung voraussetzt. Eine schematische Festlegung des Referenzzeitraumes, der bei der Negativprognose vom Arbeitgeber zugrunde zu legen ist, verbietet sich indessen bereits wegen des breiten Spektrums möglicher Krankheitsbilder. Wohl aber wird man als Richtwert eine Zeit von mindestens zwei Jahren anerkennen müssen, um sicherzustellen, dass die Prognose ausreichend fundiert ist (vergleiche Simitis, Hornung, Spiecker, Datenschutzrecht, DS-GVO mit BDSG, 1. Auflage 2019, Art. 88, Rn. 202 mit weiteren Nachweisen).

Üblicherweise werden die Arbeitsgerichte mit der Beurteilung der Rechtmäßigkeit ausgesprochener Kündigungen betraut. So entschied das Bundesarbeitsgericht in einem Urteil vom 25. April 2018, Aktenzeichen 2 AZR 6/18, dass „bei einer Kündigung wegen häufiger Kurzerkrankungen, vorbehaltlich besonderer Umstände des Einzelfalls, für die Erstellung der Gesundheitsprognose ein Referenzzeitraum von drei Jahren vor Zugang der Kündigung maßgeblich ist. Ist eine Arbeitnehmervertretung gebildet, ist auf die letzten drei Jahre vor Einleitung des Beteiligungsverfahrens abzustellen“ (vergleiche Bundesarbeitsgericht, Urteil vom 25. April 2018 – 2 AZR 6/18, BAGE 162, 327-339). Bei der Bestimmung der Dauer des Referenzzeitraumes ist also darauf abzustellen, ob es sich im Einzelfall um häufige Kurzzeiterkrankungen, eine Langzeiterkrankung oder eine dauerhafte Arbeitsunfähigkeit des Beschäftigten handelt. Während bei häufigen Kurzzeiterkrankungen im Regelfall ein längerer Zeitraum zum Nachweis einer negativen Gesundheitsprognose erforderlich sein wird, wird der Arbeitgeber bei einer dauerhaften Langzeiterkrankung bereits nach kürzerer Zeit in der Lage sein können, die Beeinträchtigungen seiner betrieblichen Interessen durch die Erkrankung des Beschäftigten einzuschätzen sowie diese darlegen und nachweisen zu können.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit griff die Argumentation des Bundesarbeitsgerichtes in der genannten Entscheidung auf und sah im konkreten Fall eine Speicherdauer von drei Jahren bei Arbeitsunfähigkeitsbescheinigungen beziehungsweise Fehlzeiten des Beschäftigten als noch angemessen an. Eine darüberhinausgehende Speicherdauer von fünf Jahren – wie von dem Arbeitgeber vorgeschlagen – wäre nach diesen Grundsätzen zu lang und müsste vom Arbeitgeber im Einzelfall besonders begründet und diese Begründung hinreichend dokumentiert werden. Für den Zeitraum der zulässigen Speicherdauer ist es dem Arbeitgeber dabei nach Art. 9 Abs. 2 Buchstabe f) DS-GVO gestattet, auch Daten besonderer Kategorie des Beschäftigten, hier dessen Gesundheitsdaten, zu verarbeiten, sofern ihm diese zulässig bekannt geworden sind. Der Beschäftigte ist dabei nicht verpflichtet, die Diagnose seiner Erkrankung dem Arbeitgeber mitzuteilen. Auch ergibt sich diese nicht aus der dem Arbeitgeber vorzulegenden ärztlichen Bescheinigung über das Bestehen der Arbeitsunfähigkeit nach § 5 Abs. 1 Satz 2 Entgeltfortzahlungsgesetz.

4.26 „Der gläserne Bauarbeiter“ – Angaben des Arbeitgebers über Beschäftigte zur Einhaltung des gesetzlichen Mindestlohnes

§ 13 Mindestlohngesetz beziehungsweise § 14 AEntG bieten keine Rechtsgrundlage für eine Datenweitergabe von Beschäftigtendaten eines Arbeitgebers an dessen Auftraggeber. Auch sonst besteht für die Bekanntgabe des vollständigen Namens, Geburtsdatums, Adresse und Pass-Nummer/ Personalausweis-Nummer der Beschäftigten durch den Arbeitgeber an einen Auftraggeber keine datenschutzrechtliche Rechtsgrundlage gemäß Art. 6 DS-GVO in Verbindung mit § 26 BDSG.

An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte sich ein Unternehmen aus dem Baugewerbe. Bei der Auftragsvergabe würden einzelne Auftraggeber die Vorlage von schriftlichen Bestätigungen der Beschäftigten des Unternehmens über den Erhalt des Mindestlohnes verlangen. Nach der dem TLfDI übersandten Muster-Bestätigung wurden folgende personenbezogenen Daten der Beschäftigten abgefragt: Name, Geburtsdatum, Adresse, Pass-Nummer/ Personalausweis-Nummer. In einer Tabelle sollten die Beschäftigten sodann je nach Zeitraum und Gewerk den gültigen Arbeitslohn ankreuzen und den sich daraus errechnenden Nettolohn für die geleisteten Arbeitsstunden nach Abzug von Steuern und Sozialversicherung bestätigen. Als letzten Satz beinhaltete die Muster-Bestätigung eine Erklärung, wonach sich die Beschäftigten mit der Weiterleitung der ausgefüllten Bestätigung an den Auftraggeber einverstanden erklären. Jeder am Bauvorhaben beteiligte Beschäftigte müsse diese Bestätigung unterschreiben. Andernfalls drohe der Auftragsverlust. Der Arbeitgeber hatte zu Recht datenschutzrechtliche Bedenken gegen eine solche umfassende Datenweiterleitung.

Wie jede andere Datenverarbeitung bedarf auch die Datenweitergabe von Beschäftigtendaten zwischen einem Auftragnehmer und Auftraggeber einer gültigen Rechtsgrundlage gemäß Art. 6 Datenschutz-Grundverordnung (DS-GVO). Zuvorderst kam im vorliegenden Fall die ausdrückliche und schriftliche *Einwilligung* der Beschäftigten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Betracht. Eine solche Einwilligung der Beschäftigten ist nach dem Willen des Gesetzgebers nicht per se ausgeschlossen, was in der Regelung des § 26

Abs. 2 Bundesdatenschutzgesetz (BDSG) zum Ausdruck kommt. Jedoch sind die Wirksamkeitsanforderungen an eine solche Einwilligung hoch; sie muss freiwillig, in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache sowie unter Hinweis auf die Widerrufsmöglichkeit abgegeben werden (Art. 7 DS-GVO). Bereits Letzteres sah die Muster-Bestätigung nicht vor. Auch konnte durch die Aufnahme von teilweise komplizierten Erläuterungen zu Gesetzen eine einfache und klare Sprache zumindest in Frage gestellt werden. Hierbei muss beachtet werden, dass die betroffenen Beschäftigten zum Teil nicht einmal der deutschen Sprache hinreichend mächtig sein werden, geschweige denn die Rechtslage zur Nachunternehmerhaftung für Mindestlöhne kennen. Auch der Standort der Einwilligung als letzter Satz in kleinerer Schriftgröße als der übrige Text führte dazu, dass die Einwilligung schnell überlesen werden konnte. Entscheidend für die negative Beurteilung der Freiwilligkeit im konkreten Sachverhalt war jedoch die Tatsache, dass den Beschäftigten, die ihre Daten an Dritte, nämlich den Auftraggeber und damit den Vertragspartner des Arbeitgebers, zur Verfügung stellen, keinerlei rechtlicher oder wirtschaftlicher Vorteil durch die Datenweitergabe entsteht, § 26 Abs. 2 Satz 2 BDSG. Ein solcher Vorteil entstünde vielmehr entweder auf Seiten des Arbeitgebers als Auftragnehmer oder auf Seiten des Auftraggebers durch eine mögliche Haftungseinschränkung, zum Beispiel durch vertragliche Regelungen mit dem Subunternehmen beziehungsweise Arbeitgeber. Nun könnte man der Auffassung sein, dass Beschäftigte und Arbeitgeber zumindest gleichgelagerte Interessen verfolgen, indem der Arbeitgeber durch die Bestätigung der Beschäftigten nicht vom Auftrag ausgeschlossen wird, was wiederum indirekt die Verdienstmöglichkeiten der Beschäftigten absichert. Eine solch weite Auslegung des „Vorteils-Begriffs“ oder der „gleichgelagerten Interessen von Arbeitgeber und Beschäftigten“ würde jedoch dazu führen, dass nahezu alle Einwilligungen von Beschäftigten als freiwillig anerkannt werden müssten, da ein irgendwie gearteter Zusammenhang zu Aufträgen des Arbeitgebers in nahezu allen Fällen gegeben sein dürfte. Eine solche weite Auslegung liefe jedoch den Interessen der Beschäftigten und deren Grundrechte auf informationelle Selbstbestimmung zuwider. Auch dürfte es an der Lebenswirklichkeit vorbeigehen, in einer solchen Konstellation, in der Arbeitgeber auf Aufträge angewiesen sind und allein hieraus indirekt eine Drucksituation für die Beschäftigten entsteht, von einer freiwilli-

gen Erklärung der Beschäftigten auszugehen. Damit schied eine Einwilligung der betroffenen Beschäftigten als Rechtsgrundlage für die Datenweitergabe aus.
Eine Rechtsgrundlage gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO („zur Erfüllung eines Vertrages“) kam ebenfalls nicht in Betracht, da die Bestimmung voraussetzt, dass die betroffene Person Vertragspartei ist. Die Beschäftigten stehen jedoch in keinem Vertragsverhältnis zum Auftraggeber.
Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO ist eine Datenverarbeitung gerechtfertigt, wenn diese „zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen“ erforderlich ist. Verantwortlicher ist der Arbeitgeber, der die Daten seiner Beschäftigten an den Auftraggeber weitergibt. § 13 Mindestlohngesetz (MiLoG) beziehungsweise § 14 Arbeitnehmerentsendegesetz (AEntG) beinhalten jedoch „lediglich“ eine Haftungsregel zu Lasten des Auftraggebers, legen dem Arbeitgeber jedoch keine rechtliche Verpflichtung zur Weiterleitung von personenbezogenen Daten der Beschäftigten an den Auftraggeber auf und können daher nicht für eine Rechtsgrundlage gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO herangezogen werden.
Schließlich scheiterte auch eine Rechtfertigung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO an der Erforderlichkeit der Übermittlung der erhobenen Daten. So gibt es für den Auftraggeber andere Möglichkeiten, sich von seinen Auftragnehmern die Einhaltung der Zahlung des gesetzlichen Mindestlohnes nachweisen zu lassen und damit seiner Haftung gemäß § 14 AEntG zu begegnen, ohne derart detaillierte Informationen von den Beschäftigten zu erfragen. Hierzu zählen Lohn- und Arbeitszeitlisten, in denen mit dem Gewerk betraute Beschäftigte teilweise anonymisiert (Anfangsbuchstaben von Vor- und Nachnamen, gegebenenfalls Geburtsdatum) geführt werden, eine Bestätigung des Auftragnehmers/ Arbeitgebers oder eine Bestätigung einer unabhängigen Stelle, zum Beispiel eines Wirtschaftsprüfers oder des Steuerberaters des Auftragnehmers.
Mangels Erforderlichkeit der Datenverarbeitung zum Zwecke der Durchführung des Beschäftigungsverhältnisses sind auch die Voraussetzungen des § 26 Abs. 1 BDSG als zentrale Norm im Beschäftigungsdatenschutz nicht erfüllt. Das Beschäftigungsverhältnis zwischen Arbeitgeber und Beschäftigtem kann auch ohne die Datenweitergabe an den Auftraggeber als Dritten gemäß Art. 4 Nr. 10 DS-GVO durchgeführt werden. Übermittlungen von Beschäftigtendaten an

Dritte sind im Regelfall nicht zur Durchführung des Beschäftigungsverhältnisses erforderlich und deshalb in den meisten Fällen nicht von § 26 Abs. 1 Satz 1 BDSG gedeckt (vergleiche Simitis, Hornung, Spiecker, Datenschutzrecht DS-GVO mit BDSG, 1. Auflage 2019, Art. 88 Rn. 188).
Im Übrigen: Sollte sich der Arbeitgeber gegenüber dem Auftraggeber vertraglich zu einer Informationspflicht hinsichtlich der Mindestlohnzahlung verpflichten (was im zu entscheidenden Fall nicht der Fall war), zum Beispiel durch monatliche Vorlage entsprechender Unterlagen oder durch Gewährung der Einsichtnahme in Lohnlisten, so gilt das Gesagte vor dem Hintergrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO) fort. Auch in einem solchen Fall dürfte der Arbeitgeber nur die Daten preisgeben, die es dem Auftraggeber ermöglichen, sein Haftungsrisiko einzuschätzen. Hierzu zählen nicht vollständige Namenslisten der Beschäftigten mit Wohnanschriften, Pass-Nummern et cetera.

4.27 Big Brother beim Bratwurstessen

Die Videoüberwachung von Gästetischen in Restaurants, Gaststätten oder auch in einem Imbiss ist unzulässig, da in diesen Bereichen Gäste miteinander kommunizieren und ihre Mahlzeiten einnehmen. Hier erwarten die Gäste, nicht überwacht zu werden. Die Überwachung dieser Bereiche stellt einen intensiven Eingriff in die Interessen der betroffenen Personen dar, welcher durch die mit der Videoüberwachung verfolgten Eigentumsinteressen des Verantwortlichen nicht gerechtfertigt werden kann. Darüber hinaus muss jeder Verantwortliche die Erforderlichkeit der Überwachung anhand der konkret festgelegten Zwecke beurteilen.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Beschwerde vor, dass auf dem Gelände eines Imbisses, welcher sich abgelegen im Thüringer Wald befindet, eine Videoüberwachung betrieben werden soll, welche erheblich in die Rechte von betroffenen Personen eingreift. Insbesondere sollten der Wanderparkplatz, Teile der öffentlichen Straße sowie der Innen- und Außenbereich des Imbisses überwacht werden.
Daraufhin wandte sich der TLfDI mit einem umfassenden Auskunftsersuchen an das für die Überwachung verantwortliche Unternehmen. Die Verantwortliche teilte mit, dass sie vier Videokameras

auf dem Gelände des Imbisses betreibt. Eine Kamera war im Innenbereich des Imbisses angebracht und filmte im vorderen Teil die Gästetische sowie die Bedientheke und den Eingang zum Imbiss. Die Kameras im Außenbereich erfassten den gesamten Wanderparkplatz sowie einen Teil der öffentlichen Straße und die im Außenbereich befindlichen Tische und Bänke. Eine vierte Kamera war an der Rückseite des Imbisses angebracht, welche auf die Fassade ausgerichtet war.

Die Zulässigkeit von Videoüberwachungen beurteilt sich nach Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO). Danach ist die Verarbeitung von personenbezogenen Daten rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen.

Wird die Videoüberwachung zur Gefahrenabwehr eingesetzt, zum Beispiel, um vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann dies grundsätzlich ein berechtigtes Interesse zum Betreiben einer Videoüberwachung darstellen, jedoch muss eine konkrete Gefahrenlage seitens des Verantwortlichen nachgewiesen werden. Dabei sind konkrete Tatsachen als Nachweis zu fordern, aus denen sich die Gefährdung ergibt (zum Beispiel durch Nennung von Beschädigungen, polizeilichen Tagebuchnummern beziehungsweise staatsanwaltschaftlichen Aktenzeichen et cetera).

Der Verantwortliche ist für die Einhaltung der Rechtmäßigkeitsvoraussetzungen seiner Datenverarbeitung verantwortlich und nach Art. 5 Abs. 2 DS-GVO zur „Rechenschaft“ verpflichtet, das heißt, er muss die Einhaltung der Rechtmäßigkeitsvoraussetzungen nachweisen können. In diesem Fall konnte der Verantwortliche entsprechende Vorkommnisse benennen, welche außerhalb der Geschäftszeiten des Imbisses stattgefunden haben. Unter anderem wurden hier Sachbeschädigungen und ein Einbruch benannt.

Neben dem berechtigten Interesse muss die Überwachung für den verfolgten Zweck erforderlich sein, das heißt, sie muss geeignet sein und es darf kein anderes, gleich wirksames Mittel zur Verfügung stehen. Darüber hinaus muss auch das „Wie“ des Einsatzes der Videotechnik Gegenstand der Erforderlichkeitsprüfung sein, insbesondere der zeitliche und räumliche Umfang sowie die technische und organisatorische Ausgestaltung. Im vorliegenden Fall wurden zwar Tatsachen vorgetragen, die eine Gefährdungslage begründen können, jedoch fan-

den die Vorkommnisse nur außerhalb der Geschäftszeiten des Imbisses statt. Nach Einschätzung des TLfDI lag daher keine Erforderlichkeit einer Videoüberwachung innerhalb der Geschäftszeiten vor. Etwaige Vorkommnisse, welche auch eine Gefährdungslage während der Geschäftszeiten begründen könnte (zum Beispiel ein Überfall), wurden seitens des Verantwortlichen nicht dargelegt. Selbst wenn ein solcher Vorfall stattgefunden hätte, wäre eine Überwachung lediglich auf den vorderen Bereich der Bedientheke zu beschränken. Auch die Überwachung des kompletten Wanderparkplatzes und der öffentlichen Straße war für die vom Verantwortlichen verfolgten Zwecke nicht erforderlich. Hinsichtlich des Eigentumsschutzes ist es ausreichend, nur die Bereiche des Imbisses selbst zu überwachen.
Als letzter Prüfungsschritt muss eine einzelfallorientierte Interessenabwägung durchgeführt werden, das heißt, es ist anhand des konkreten Sachverhalts zu beurteilen, wie gewichtig die mit der Videoüberwachung verfolgten Interessen des Verantwortlichen sind und inwieweit diese durch die Videoüberwachung tatsächlich gefördert werden. Zum anderen ist zu prüfen und unter Berücksichtigung der vernünftigen Erwartungen des Betroffenen zu gewichten, inwieweit die Überwachung in schutzwürdige Interessen, Grundrechte und Grundfreiheiten eingreift und welche möglichen Folgen für Betroffene daraus resultieren können. Ob vernünftige Erwartungen bestehen, beurteilt sich danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert wird oder nicht.
Vorliegend wurden durch die Überwachung eine Vielzahl von Personen, welche den Parkplatz und den Imbiss im Rahmen ihrer Freizeitgestaltung aufsuchen, unter Generalverdacht gestellt, was einen intensiven Eingriff in deren Rechte darstellte. Zudem können Personen erwarten, auf einem Wanderparkplatz und auf der öffentlichen Straße im Rahmen ihrer Freizeit nicht ständig überwacht zu werden. Weiterhin fanden auf dem dortigen Gelände Feste und Veranstaltungen statt, was den Eingriff in die Rechte der betroffenen Personen noch verstärkte.
Die Überwachung von Ess- und Aufenthaltsbereichen in der Gastronomie ordnet die Rechtsprechung ebenfalls dem Freizeitbereich zu (AG Hamburg, Urteil vom 22. April 2008, Az.: 4 C 134/08). Dort halten sich Gäste typischerweise über längere Zeit auf, sie essen, trinken und unterhalten sich. Hier sind die Persönlichkeitsrechte der Gäste besonders zu schützen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gast-

stättenbesucher und greift intensiv in deren Rechte ein, so dass solche Bereiche regelmäßig nicht überwacht werden dürfen.
Da seitens des Verantwortlichen im Verwaltungsverfahren kein Einsehen bezüglich der geforderten Maßnahmen seitens des TLfDI zu erreichen war, erging letztendlich ein Bescheid nach Art. 58 Abs. 2 Buchstabe d) und f) DS-GVO, wonach es dem TLfDI gestattet ist, eine vorübergehende oder endgültige Beschränkung der Verarbeitung einschließlich eines Verbots zu verhängen und den Verantwortlichen anzuweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der Verordnung zu bringen. Es wurde angeordnet, dass die Überwachung des Imbisses nur noch außerhalb der Geschäftszeiten zu erfolgen hat und der Wanderparkplatz und die öffentliche Straße von der Überwachung auszunehmen war.

4.28 E-Mail-Kommunikation nur noch Ende-zu-Ende verschlüsselt?

Für die Übermittlung von personenbezogenen Daten mittels elektronischer Kommunikation enthält die DS-GVO keine konkreten Vorgaben. Hier muss auf allgemeine Vorgaben hinsichtlich der Sicherheit der Verarbeitung zurückgegriffen werden (Art. 5, 32 DS-GVO). Die DSK hat zur Konkretisierung eine entsprechende Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ herausgegeben. Die vorzunehmende Art der Verschlüsselung von personenbezogenen Daten wird anhand einer Risikoabschätzung beurteilt.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde des Kunden eines Thüringer Energieunternehmens. Grund hierfür war eine E-Mail des Unternehmens an seine Kunden, in der ein Schreiben enthalten war, welches unter anderem den Namen, die Anschrift, die Zählernummer des Stromzählers, die Mess- und Marktlokationsnummer der Verbrauchsstelle des Kunden enthielt. Inhaltlich ging es lediglich um die Wiederinbetriebnahme der Verbrauchsstelle. Weitere Einzelheiten sollten mit der Zweigstelle des Unternehmens telefonisch abgeklärt werden. Fraglich war, ob das Unternehmen auf diesem Weg personenbezogene Daten übermitteln durfte.

Im Rahmen des Auskunftsverlangens des TLfDI teilte das verantwortliche Unternehmen mit, dass es seinen Kunden mehrere Kontaktmöglichkeiten anbietet (Telefon, E-Mail, Fax et cetera). Standardmäßig erfolge die Kontaktaufnahme jedoch postalisch oder telefonisch. Die Kommunikation per E-Mail erfolge erst durch eine entsprechende initiale Kontaktaufnahme durch den Kunden. Hier würden jedoch lediglich einfache Fragestellungen oder Sachverhalte ohne die Preisgabe von besonders schützenswerten Daten übermittelt. Eine gesonderte Einwilligung in diesen Kommunikationsweg hole das Unternehmen nicht ein. Selbst wenn durch das Unternehmen eine Einwilligung in die unverschlüsselte Kommunikation per E-Mail eingeholt worden wäre, würden die Verarbeitungstätigkeiten hierdurch nicht rechtmäßig. Insoweit sind immer die zu treffenden technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik seitens des Verantwortlichen zu beachten.
Hierfür seien entsprechende Maßnahmen nach Art. 32 Datenschutz-Grundverordnung (DS-GVO) durch die Verantwortliche zum Schutz der Daten der Kunden getroffen worden. Insbesondere unterstütze deren Mail-Server bei der Versendung an Empfänger und dem Empfang von E-Mails von Absendern außerhalb des Unternehmens das Verschlüsselungsprotokoll TLS (Transport Layer Security). Sofern der Mail-Server des Empfängers beziehungsweise Absenders dieses Protokolls ebenfalls unterstützt, sei eine Transportverschlüsselung gegeben. Darüber hinaus bestehe die Möglichkeit, angehängte Dokumente an einer E-Mail mit einem Passwortschutz zu versehen und so eine Verschlüsselung zu gewährleisten. Zudem sei es in dem Unternehmen möglich, E-Mails über eine Ende-zu-Ende-Verschlüsselung zu sichern.
Hinsichtlich der elektronischen Kommunikation enthält die DS-GVO keine konkreten Vorgaben. Hier muss auf Art. 5 Abs. 1 Buchstabe f), Art. 32 Abs. 1 Buchstabe a) und Buchstabe b) DS-GVO bezüglich allgemeiner Vorgaben hinsichtlich der Sicherheit der Verarbeitung zurückgegriffen werden. Welche konkreten Maßnahmen die DS-GVO mit der Verschlüsselung anstrebt, wird in Art. 32 DS-GVO nicht deutlich. Insbesondere werden keine Vorgaben zur Art der Verschlüsselung bei einer Datenübermittlung gemacht. Entsprechend der Vorgaben der seit dem 12. Mai 2020 beschlossenen Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (abrufbar unter

https://www.datenschutzkonferenz-online.de/orientierungshilfen.html) ist seitens des Verantwortlichen eine Risikoeinschätzung bei dem Versand von E-Mails vorzunehmen. Handelt es sich um ein normales Risiko, also werden keine sensiblen Daten wie zum Beispiel Bank- und Abrechnungsdaten, übermittelt, ist eine Transportverschlüsselung dem Stand der Technik ausreichend, wenn diese nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik (hier BSI TR 02102-2) verwendet wird. Der Einsatz von Transportverschlüsselung bietet einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht. Die Transportverschlüsselung reduziert jedoch lediglich die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Zudem prüfen die beteiligten Provider in der Regel nach Eingang einer Nachricht diese unmittelbar auf Schadsoftware. Dies bedeutet, dass dort jede Mail für einen kurzen Moment automatisch geprüft wird, bevor sie weitergeleitet oder für den Abruf gespeichert wird. Durch eine Ende-zu-Ende-Verschlüsselung ist es hingegen möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern (siehe Beitrag 2.10). Laut den Angaben des Unternehmens wurde eine den Standards des BSI entsprechende Transportverschlüsselung (TLS) beim Versand und Empfang von E-Mails eingesetzt.
Das per E-Mail versandte Schreiben enthielt den Namen und die Anschrift des Kunden sowie pseudonymisierte Daten, welche nur durch den Energielieferanten entschlüsselt werden könnten (Messlokationsnummer und Marktlokation sowie Zählernummer). Weitere Daten, welche ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person begründen könnten, waren in dem Schreiben an den Kunden nicht enthalten. Eine Ende-zu-Ende-Verschlüsselung der E-Mail und des Anhangs war daher aus Sicht des TLfDI nicht erforderlich und die eingesetzte Transportverschlüsselung ausreichend.
Bei dem hier geprüften Unternehmen lagen hinsichtlich der elektronischen Kommunikation ausreichend getroffene Maßnahmen zur Verschlüsselung vor, so dass ein Datenschutzverstoß seitens des TLfDI

bei der Übermittlung der personenbezogenen Daten des betreffenden Beschwerdeführers nicht festgestellt werden konnte.

4.29 Kleingartensiedlung unter Beobachtung

Bei der Videoüberwachung des eigenen Grundstückes ist in bestimmten Fällen das Datenschutzrecht zu beachten. Insbesondere gilt dies, sofern der öffentlich zugängliche Bereich, wie zum Beispiel der Eingang, überwacht wird. Dienen die Kameras auch dazu, etwaige Beweissicherungsinteressen zu verfolgen, geht die Datenverarbeitung über den persönlich familiären Bereich hinaus, so dass die so genannte Haushaltsausnahme in diesen Fällen nicht zur Anwendung gelangt.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über eine umfassende Videoüberwachung eines Kleingartens in einer Kleingartensiedlung. Die Kameras sollten so ausgerichtet sein, dass die Nachbargärten sowie der Hauptweg zu den einzelnen Kleingärten erfasst würden.
Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen an die Kleingartennutzer beziehungsweise -pächter. Diese teilten mit, dass sie fünf Kameras in dem Kleingarten betreiben. Sämtliche Videokameras waren auf den eigenen Gartenbereich ausgerichtet. Nachbargrundstücke und der Hauptweg konnten auch bei nicht vorhandener Vegetation im Winter nicht beobachtet werden. Es wurde mit den Kameras der Zugang zu der Gartenlaube überwacht. Als Zweck für die Überwachung gaben die Besitzer an, dass es in der Vergangenheit zu Sachbeschädigungen in ihrem Garten gekommen sei und zudem in dem letzten Jahr zu Einbrüchen in den Nachbargärten kam.
Zunächst musste gegenüber den Nutzern des Kleingartens klargestellt werden, dass die Privilegierung des Art. 2 Abs. 2 Buchstabe c) Datenschutz-Grundverordnung (DS-GVO) hinsichtlich der durch sie betriebenen Videoüberwachung nicht eingreift. Danach findet die DS-GVO bei der Verarbeitung von personenbezogenen Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten keine Anwendung. Videoüberwachungen gehen dann über den persönlichen und familiären Bereich hinaus, sofern sie öffentlich zugängliche Bereiche , wie zum Beispiel Eingänge, überwachen. Auch die Überwachung über das eigene Grundstück hinaus, also auch die Überwachung von Nachbargrundstücken, fällt unter die An-

wendung des Datenschutzrechts. Für die datenschutzrechtliche Beurteilung sind weiterhin die verfolgten Zwecke zu berücksichtigen. Eine Privilegierung ist dann abzulehnen, wenn Videoaufzeichnungen zur Schaffung von Beweismitteln angefertigt werden, um diese für eine spätere Rechtsverfolgung zu verwenden. Dabei kommt es nicht darauf an, wie wahrscheinlich eine Nutzung zu diesem Zweck ist, es reicht aus, dass die Aufzeichnung auch zu diesem Zweck erfolgt.
Da die angebrachten Videokameras dem Zweck dienten, etwaige Beweise bei einem Einbruch oder bei Sachbeschädigungen zu sichern und auch der Zugang zur Gartenlaube überwacht wurde, konnte die Privilegierung des Art. 2 Abs. 2 Buchstabe c) DS-GVO nicht eingreifen. Die Videoüberwachung musste daher den geltenden Bestimmungen des Datenschutzrechts entsprechen.
Die Rechtmäßigkeitsvoraussetzungen für eine Videoüberwachung ergeben sich grundsätzlich aus Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Danach ist die Verarbeitung von personenbezogenen Daten rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.
Im vorliegenden Fall war ein berechtigtes Interesse seitens der Kleingartennutzer zum Betreiben der Videokameras gegeben. Auch der räumliche Umfang der Videoüberwachung, welche nur auf das eigene Grundstück ausgerichtet war, war nicht zu beanstanden. Überwiegende schutzwürdige Belange von betroffenen Personen waren hier ebenfalls nicht erkennbar. Es wurde allerdings seitens des TLfDI die Anpassung der Speicherdauer verlangt. Die Kleingartennutzer hatten eine regelmäßige Speicherdauer von zwei Wochen eingestellt. Personenbezogene Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks der Überwachung nicht mehr erforderlich sind, Art. 17 Abs. 1 Buchstabe a) DS-GVO. Bei der hier betriebenen Videoüberwachung wäre eine Löschung der Aufnahmen vorzunehmen, sofern ein Vorfall wie ein Einbruch oder eine Sachbeschädigung nicht stattgefunden hat. Wann dies bei einem genutzten Kleingarten der Fall ist, kann variieren. Sofern die Gartenbesitzer in den Sommermonaten mehrmals in der Woche den Garten aufsuchen, sollte die Speicherdauer auf 48 Stunden verkürzt werden, da innerhalb dieses Zeitraums etwaige Vorfälle in dem Garten feststellbar sind. Bei einer längeren Abwesenheit durch Urlaub oder auch in den Wintermonaten ist die Anpassung der Speicherdauer für einen längeren Zeitraum möglich.

Eine regelmäßige Speicherdauer von zwei Wochen war jedoch nicht gerechtfertigt. Weiter wurde die Anbringung von Hinweisschildern, welche den Vorgaben der Datenschutz-Grundverordnung entsprechen, gefordert. Dies setzten die Kleingartennutzer umgehend um, so dass keine weiteren Forderungen seitens des TLfDI hinsichtlich der Videoüberwachung mehr bestanden.

5. Entschließungen und Beschlüsse

© ilro - Paragraph und Fragezeichen - fotolia.com

5.1 Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 3. April 2020

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.
Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der

Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.
Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.
Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

- Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.
- Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.
- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder – wie eine vorherige Anonymisierung – sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung –**außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müs-

sen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu l**öschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.
- Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. **Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

5.2 Polizei 2020 – Risiken sehen, Chancen nutzen!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 16. April 2020

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten „fachlichen Bebauungsplan“ für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.
Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

1. Umfassende Bestandsaufnahme

Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken

Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern

des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerte- und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste“ zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung“, ein „Basisdienst Datenqualität“ und ein „Basisdienst Aufsicht und Kontrolle“.

5.3 Registermodernisierung verfassungskonform umsetzen!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 26. August 2020

Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz – RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll u. a. eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.
Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12.09.2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.
Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potential der möglichen missbräuchlichen Verwendung.
So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und

zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks. Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.
Die Datenschutzkonferenz hatte demgegenüber „sektorspezifische" Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.
Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf „rechtliche, technische und organisatorische Komplexität" abgelehnt.
Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den „Eilbedarf" unter den Tisch fallen zu lassen.
Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

5.4 Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 1. September 2020

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen. Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden. Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.
Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.
Erst ein Jahr nach dem Start der EPA, d. h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte (Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d. h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs. 164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

5.5 Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22. September 2020

Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[1] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.
Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters. Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[2] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese

[1] Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

[2] PwC Strategy & (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten.“ Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.
Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,
- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und
- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:

- Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.
- Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.
- Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:
   - Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.
3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:
   - Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.
4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:
   - Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten

diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.
- Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:
   - Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

5.6 Datenschutz braucht Landgerichte auch erstinstanzlich

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22. September 2020

Mit dem „*Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens*“ (BR-Drs. 107/20 (B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen nach der Datenschutz-Grundverordnung (DSGVO) über 100.000 Euro streichen. Selbst über Geldbußen in dieser Höhe sollen künftig die Amtsgerichte entscheiden.
Das Ziel der Effektivierung des Bußgeldverfahrens wird mit dem geplanten Gesetz jedoch nicht erreicht werden. Der Gesetzentwurf verkennt in eklatanter Weise die besondere wirtschaftliche, technische und rechtliche Komplexität von DSGVO-Geldbußen. Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte zudem nicht etwa entlasten, sondern noch stärker als bisher belasten.
Das Sanktionsrecht der DSGVO ist – anders als der Bundesrat unterstellt – mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchstrelevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Datenschutz-Ordnungswidrigkeiten mit Geldbußen über 100.000 Euro weisen wirtschaftlich und technisch eine besondere Komplexität auf und bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind viel eher mit Wirtschaftsstrafsachen vergleichbar, die ohnehin den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DSGVO am Kartellrecht orientiert. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Abs. 2 Satz 1 Bundesdatenschutzgesetzes (BDSG) zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der

Strafkammern als sog. große Bußgeldkammern entsprechend § 76 GVG vorsieht.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert daher die Beibehaltung der landgerichtlichen Zuständigkeit für DSGVO-Geldbußen über 100.000 Euro und warnt vor einer Streichung der Vorschrift und deren Folgen.

5.7 Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 25. November 2020

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.
Eine sichere und vertrauenswürdige Verschlüsselung ist essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangsgesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.
Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das „Schrems II“-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten. Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.
Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Art. 7 GRCh geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Art. 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Art. 10 GG und ergänzend durch das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.
Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.
Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integrer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integrer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestre-

ben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

5.8 Betreiber von Webseiten benötigen Rechtssicherheit Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 25. November 2020

Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie[3] vollständig und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) umzusetzen.
Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt hat.[4] Das Urteil des Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 – „Planet49“) verstärkt nach Auffassung der DSK den seit langem bestehenden, dringenden Handlungsbedarf.
Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018“ den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der Datenschutz-Grundverordnung (DSGVO) nicht mehr anwendbar sind.
Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.[5]

---

[3] Richtlinie 2002/58/EG in der letzten Änderung durch die Richtlinie 2009/136/EU

[4] Siehe Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20150205_en_Entschliessung_Cookies.pdf

[5] Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“, abrufbar unter: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html), Orientierungshilfe für Anbieter von Telemedien (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Abs. 3 Telemediengesetz (TMG) wäre ein solches Vorgehen dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 ePrivacy-Richtlinie legt der BGH § 15 Abs. 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der BGH der Vorabentscheidung des Europäischen Gerichtshofes gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.
Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.
Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacy-Richtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene weitgehend abschließend durch die Datenschutz-Grundverordnung geregelt. Art. 5 Abs. 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Abs. 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.
§ 15 Abs. 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der

Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Abs. 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste u. a. in Bezug auf „Cookies“ rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen.

5.9 Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 25. November 2020

Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicherheitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.
Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs-und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.
Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehör-

den des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.
Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vgl. BVerfG, o. g. Beschluss vom 27. Mai 2020, Rn. 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.

5.10 Einwilligungsdokumente der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 15. April 2020

Aus Sicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestehen gegen den bundesweiten Einsatz der Einwilligungsdokumente der Medizininformatik-Initiative in der Version 1.6b, bestehend aus einer Patienteninformation und einer Einwilligungserklärung, sowie der zugehörigen Handreichung in der Version 0.9b keine Bedenken, unter der Voraussetzung, dass in den Einwilligungsdokumenten auf die Verarbeitung genetischer Daten aus Biomaterialien und insbesondere das damit verbundene Risiko der Rückverfolgbarkeit explizit hingewiesen wird, die Wahrung des jederzeitigen Widerrufsrechts trotz der Übertragung des Eigentums an Biomaterialien klarer zum Ausdruck kommt und Patienten auf die Möglichkeit hingewiesen werden, sich bei einem E-Mail-Verteiler zu registrieren, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert. In der Handreichung ist außerdem die Passage zu streichen, in der darauf hingewiesen wird, dass zukünftig die Datenübermittlung in Drittstaaten zulässig sein soll.
Zur Umsetzung dieser Anforderungen in der Patienteninformation wird vorgeschlagen:

- Unter 3.2 im ersten Absatz nach Satz 2 einzufügen: "In Biomaterialien kann Ihre Erbsubstanz in Form genetischer Daten enthalten sein. Insofern sind insbesondere die unter 1.4 beschriebenen Risiken für genetische Daten zu beachten. Hierzu zählt auch ein erhöhtes Risiko einer Rückverfolgbarkeit Ihrer Person anhand dieser Daten."
- Unter 3.3 im ersten Absatz nach Satz 2 einzufügen: "Ihr Recht, über die Verarbeitung Ihrer personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsübertragung unberührt. Trotz Eigentumsübertragung können Sie Ihre Einwilligung in die Datenverarbeitung jederzeit widerrufen (siehe Punkt 6) und die Vernichtung Ihrer Biomaterialien verlangen."

– Zudem ist in der Einwilligung und in der Patienteninformation jeweils an geeigneter Stelle auf die Möglichkeit der Registrierung bei einem E-Mail-Verteiler hinzuweisen, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert.

Ergänzend sollte in der Einwilligungserklärung in dem Kasten unter 3.3 als zweiter Satz aufgenommen werden: "Mein Recht, über die Verarbeitung meiner dem Biomaterial zu entnehmenden personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsübertragung unberührt (siehe Punkt 3.3 der Patienteninformation)."

Als redaktionelle Korrektur wird zudem empfohlen, in der Einwilligungserklärung unter 1.1 zum Stichwort der Codierung auch auf Punkt 1.3 der Patienteninformation zu verweisen, da die Codierung dort beschrieben wird.

5.11 Vorabwidersprüche bei StreetView und vergleichbaren Diensten

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 12. Mai 2020

Für die Veröffentlichung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche an den öffentlichen Straßenraum angrenzen, kann im Rahmen von StreetView und ähnlichen Diensten Art. 6 Abs. 1 Unterabsatz 1 lit. f DSGVO als Rechtsgrundlage in Betracht kommen. Dabei dürfen nur die personenbezogenen Daten veröffentlicht werden, die für die Zweckerreichung zwingend erforderlich sind, so sind Merkmale, die die Identifizierung einer Person ermöglichen, insbesondere Gesichter und KFZ-Kennzeichen, unkenntlich zu machen. Dies ergibt sich bereits aus Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung). Zudem hat der Anbieter vor Beginn der Aufnahmen die Öffentlichkeit in geeigneter Weise zu informieren.
Im Rahmen der Interessenabwägung ist ein Verlangen betroffener Personen auf Unkenntlichmachung personenbezogener Daten zu berücksichtigen. Dieses Verlangen kann zumindest ab dem Zeitpunkt der Anfertigung der Aufnahmen durch den Dienst wahrgenommen werden und umfasst auch Abbildungen von Häuserfassaden und privaten Grundstücksbereichen. Art. 21 DS-GVO bleibt unberührt.
Das Verlangen auf Unkenntlichmachung nach Art. 17 Abs. 1 DS-GVO und der Widerspruch nach Art. 21 DS-GVO müssen sowohl online als auch postalisch eingelegt werden können. Auf diese Rechte muss ausdrücklich hingewiesen werden.

5.12 Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 12. Mai 2020

Google Analytics ist eines der weitest verbreiteten Tools für Website-Betreiber (Anwender). Mit Hilfe dieses Tools lassen sich umfassende statistische Auswertungen der Webseitennutzung vornehmen. Aus diesem Grund besteht ein großer Beratungsbedarf hinsichtlich des Einsatzes von Google Analytics.
Die Datenschutzaufsichtsbehörden haben vor dem Hintergrund des neuen Rechtsrahmens mit Geltung der DS-GVO den Einsatz von Google Analytics neu bewertet. Ältere Auffassungen der Datenschutzaufsichtsbehörden, die unter Berücksichtigung der Rechtslage vor dem 25.05.2018 kommuniziert wurden, gelten damit als überholt.[6]
Im Folgenden handelt es sich keinesfalls um eine abschließende Beurteilung. Die folgenden Ausführungen stellen eine Ergänzung der Orientierungshilfe für Anbieter von Telemedien[7] dar und betreffen lediglich die häufigsten Fragestellungen beim Einsatz von Google Analytics. Die folgenden Ausführungen stellen keine Empfehlung zum Einsatz von Google Analytics dar, sondern beschreiben nur die datenschutzrechtlichen Mindestanforderungen, die von Seitenbetreibern nach derzeitigem Stand zwingend eingehalten werden müssen.

Die Auffassungen der Datenschutzaufsichtsbehörden stehen unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss und der Rechtsprechung des EuGH.
Die Ausführungen gelten für den Fall, dass der Anwender von Google-Analytics die von Google derzeit[8] empfohlenen Standardein-

[6] Dies gilt insbesondere für die Veröffentlichung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, „Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen“.
[7] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
[8] Stand: 11.03.2020.

stellungen nutzt. Für den Fall, dass der Anwender von Google Analytics von den empfohlenen Einstellungen abweicht und/oder ergänzende Funktionen verwendet (z. B. Google Analytics 360) oder Google die Verarbeitung oder die vertraglichen Grundlagen ändert, wird auf die von den deutschen Datenschutzaufsichtsbehörden veröffentlichten Ausführungen der Orientierungshilfe für Anbieter von Telemedien verwiesen.

I. Personenbezogene Daten

Beim Einsatz von Google Analytics werden immer personenbezogene Daten der Nutzer verarbeitet.
In den Google Analytics-Hilfen[9] erläutert Google, dass Nutzungsdaten keine „personenidentifizierbaren Informationen“ seien. Diese Auffassung steht nicht nur im Widerspruch zur Definition des Begriffs „personenbezogene Daten“ in Art. 4 Nr. 1 der DS-GVO, sondern ist auch missverständlich, da Google im Weiteren Folgendes ausführt: *„Bitte beachten Sie, dass Daten, die Google nicht als personenidentifizierbare Informationen einstuft, im Rahmen der DS-GVO als personenbezogene Daten gelten können.“*
Die Datenschutzaufsichtsbehörden weisen daher ausdrücklich darauf hin, dass es sich bei den mit Google Analytics verarbeiteten Daten (Nutzungsdaten und sonstige gerätespezifische Daten, die einem bestimmten Nutzer zugeordnet werden können) um personenbezogene Daten i. S. d. DS-GVO handelt.

II. Verhältnis zwischen Google Analytics-Anwender und Google

Google hat die Verarbeitungsprozesse von Google Analytics fortlaufend angepasst. Dies hat dazu geführt, dass Google Analytics nicht mehr nur ein Tool zur statistischen Analyse (Reichweitenmessung) ist, sondern dem Anwender eine Vielzahl an weiteren Funktionen bietet, mit denen der Anwender verschiedene Zwecke verfolgen kann.
Nach Auffassung der Datenschutzaufsichtsbehörden ist die Verarbeitung im Zusammenhang mit Google Analytics keine Auftragsverarbeitung gemäß Art. 28 DS-GVO. Nach Art. 4 Nr. 7, Art. 28 Abs. 10 DS-GVO hat der Verantwortliche die Zwecke und Mittel der Verar-

[9] Abrufbar unter der URL: https://support.google.com/analytics/answer/7686480 [Stand: 27.09.2019].

beitung selbst zu bestimmen. Daraus folgt die Pflicht des Auftragsverarbeiters, die Daten ausschließlich auf Weisung des Verantwortlichen zu verarbeiten (Art. 29 DS-GVO). Beim Einsatz von Google Analytics bestimmt der Website-Betreiber nicht allein über die Zwecke und Mittel der Datenverarbeitung. Diese werden vielmehr zum Teil ausschließlich von Google vorgegeben, sodass Google insoweit selbst verantwortlich ist, und vom Seitenbetreiber vertraglich akzeptiert. Die Verarbeitung beim Einsatz von Google Analytics stellt einen einheitlichen Lebenssachverhalt dar, in dem die verschiedenen Aspekte der Verarbeitung nur als Ganzes einen Sinn ergeben. Dies hat zur Folge, dass die Beteiligten innerhalb einer Verarbeitungstätigkeit nicht ihre Rolle als Auftragsverarbeiter und/oder Verantwortlicher wechseln können.

Zwar bietet Google weiterhin einen Vertrag zur Auftragsverarbeitung an, stellt aber zusätzlich in den „Google Measurement Controller-Controller Data Protection Terms“[10] klar, dass für bestimmte Verarbeitungsprozesse Google und der Anwender (Website-Betreiber) getrennt verantwortlich seien. Zudem stellt Google in den Nutzungsbedingungen[11] klar, dass Google die Daten für eigene Zwecke, insbesondere auch zum Zweck der Bereitstellung seines Webanalyse-und Trackingdienstes, verarbeite. Gemäß Artikel 28 Abs. 10 DS-GVO handelt es sich bei Google damit nicht mehr um einen Auftragsverarbeiter.

Unter Berücksichtigung der aktuellen Rechtsprechung des EuGH sind Google und der Google-Analytics-Anwender gemeinsam für die Datenverarbeitung verantwortlich, sodass die Anforderungen des Art. 26 DS-GVO zu beachten sind.

III. Rechtsgrundlage

Der Einsatz von Google Analytics kann in aller Regel nicht auf Art. 6 Abs. 1 lit. b) DS-GVO gestützt werden, da der Einsatz von Google Analytics nicht zur Vertragserfüllung zwischen Website-Betreiber und Nutzer erforderlich ist.

---

[10] Das „Google Measurement Controller-Controller Data Protection Terms“, abrufbar unter: https://support.google.com/analytics/answer/9012600,Fassung vom 4. November 2019, Ziff. 4, gilt u. a. für den Fall, dass Google-Produkte und -Dienste in den Einstellungen zur Datenfreigabe aktiviert sind.

[11] Abrufbar unter: https://marketingplatform.google.com/about/analytics/terms/de/, Fassung vom 17. Juni 2019, Ziff. 6, 7.

Der Einsatz von Google Analytics ist *in der Regel* auch nicht nach Art. 6 Abs. 1 lit. f) DS-GVO rechtmäßig. Angesichts der konkreten Datenverarbeitungsschritte beim Einsatz von Google Analytics überwiegen die Interessen, Grundrechte und Grundfreiheiten der Nutzer regelmäßig die Interessen der Website-Betreiber. Insbesondere rechnet der Nutzer vernünftigerweise nicht damit, dass seine personenbezogenen Daten mit dem Ziel der Erstellung personenbezogener Werbung und der Verknüpfung mit den aus anderen Zusammenhängen gewonnenen personenbezogenen Daten an Dritte weitergegeben und umfassend ausgewertet werden.[12] Dies geht weit über das hinaus, was im Rahmen des Art. 6 Abs. 1 lit. f) DS-GVO zulässig ist.[13] Die Situation weicht insoweit erheblich von dem Fall einer Statistik-Funktion auf der eigenen Website oder mittels Auftragsverarbeitung ab.
Google verpflichtet in den vertraglichen Regelungen den Anwender von Google Analytics, unter bestimmten Voraussetzungen für den Einsatz des Dienstes eine Einwilligung der Besucher der Webseite einzuholen.[14] Die Datenschutzaufsichtsbehörden weisen ausdrücklich darauf hin, dass es für den rechtmäßigen Einsatz von Google Analytics nicht auf die vertraglichen Vereinbarungen zwischen Google und dem Anwender ankommt. Die Rechtmäßigkeit richtet sich ausschließlich nach dem Gesetz.
Im Ergebnis ist ein rechtmäßiger Einsatz von Google Analytics in der Regel nur aufgrund einer wirksamen Einwilligung der Webseitenbesuchenden gem. Art. 6 Abs. 1 lit. a), Art. 7 DS-GVO möglich.

IV. Maßnahmen

Sofern Website-Betreiber nicht auf alternative und datensparsame Werkzeuge zur Reichweitenmessung ausweichen, sondern weiterhin Google Analytics verwenden, sind insbesondere folgende Maßnahmen umzusetzen:

---

[12] Datenschutzerklärung von Google unter: https://policies.google.com/privacy, Fassung wirksam ab dem 15. Oktober 2019, unter der Überschrift „Messung der Leistung“.
[13] Nähere Erläuterungen in der „Orientierungshilfe für Anbieter von Telemedien“.
[14] Vgl. „Nutzungsbedingungen“, abrufbar unter: https://marketingplatform.google.com/about/analytics/terms/de/, Fassung vom 17. Juni 2019; „Richtlinienanforderungen für Google Analytics-Werbefunktionen“, abrufbar unter: https://support.google.com/analytics/answer/2700409, Fassung vom 16. Dezember 2016; „Richtlinie zur Einwilligung der Nutzer in der EU“, abrufbar unter: https://www.google.com/about/company/user-consent-policy.html,ohne Datum, zuletzt abgerufen am 23. Januar2020.

1) Einholung einer informierten, freiwilligen, aktiven und vorherigen Einwilligung der Nutzer

Eine Einwilligung ist nur wirksam, wenn die Anforderungen gem. Art. 4 Nr. 11, Art. 7 DS-GVO und ggf. Art. 8 DS-GVO erfüllt sind. Das bedeutet insbesondere:

- Website-Betreiber müssen sicherstellen, dass die Einwilligung die **konkrete Verarbeitungstätigkeit** durch die Einbindung von Google Analytics und damit verbundene Übermittlungen des Nutzungsverhaltens an Google LLC erfasst.
- In der Einwilligung muss **klar und deutlich** beschrieben werden, dass die Datenverarbeitung im Wesentlichen durch Google erfolgt, die Daten nicht anonym sind, welche Daten verarbeitet werden und dass Google diese zu beliebigen eigenen Zwecken wie zur Profilbildung nutzt sowie mit anderen Daten wie eventueller Google-Accounts verknüpft. Ein bloßer Hinweis wie z. B. „diese Seite verwendet Cookies, um Ihr Surferlebnis zu verbessern“ oder „verwendet Cookies für Webanalyse und Werbemaßnahmen“ ist nicht ausreichend, sondern irreführend, weil die damit verbundenen Verarbeitungen nicht transparent gemacht werden.
- Nutzer müssen **aktiv** einwilligen, d. h. die Zustimmung darf nicht unterstellt und ohne Zutun des Nutzers voreingestellt sein. Ein Opt-Out-Verfahren reicht nicht aus, vielmehr muss der Nutzer durch aktives Tun (z. B. Anklicken eines Buttons) seine Zustimmung zum Ausdruck bringen. Google muss ausdrücklich als Empfänger der Daten aufgeführt werden. Vor einer aktiven Einwilligung des Nutzers dürfen keine Daten erhoben oder Elemente von Google-Websites nachgeladen werden. Auch das bloße Nutzen einer Website (oder einer App) stellt keine wirksame Einwilligung dar.
- **Freiwillig** ist die Einwilligung nur, wenn die betroffene Person Wahlmöglichkeiten und eine freie Wahl hat. Sie muss eine Einwilligung auch verweigern können, ohne dadurch Nachteile zu erleiden. Die Koppelung einer vertraglichen Dienstleistung an die Einwilligung zu einer für die Vertragserbringung nicht erforderlichen Datenverarbeitung kann gemäß Art. 7 Abs. 4 DS-GVO dazu führen, dass die Einwilligung nicht freiwillig und damit unwirksam ist.

Um die Anforderungen einer wirksamen Einwilligung auf Websites oder in Apps umzusetzen, sind folgende Gestaltungshinweise zu beachten:

- **Klare, nicht irreführende Überschrift** – bloße „Respektbekundungen“ bezüglich der Privatsphäre reichen nicht aus. Es empfehlen sich Überschriften, in denen auf die Tragweite der Entscheidung eingegangen wird, wie beispielsweise *„Datenverarbeitung Ihrer Nutzerdaten durch Google“*.
- **Links** müssen **eindeutig** und unmissverständlich beschrieben sein – wesentliche Elemente/Inhalte insbesondere einer Datenschutzerklärung dürfen nicht durch Links verschleiert werden.
- Der **Gegenstand** der Einwilligung muss **deutlich gemacht** werden: Anwender von Google Analytics müssen deutlich machen, für welchen Zweck Google Analytics verwendet wird, dass die Nutzungsdaten von Google LLC verarbeitet werden, diese Daten in den USA gespeichert werden, sowohl Google als auch staatliche Behörden Zugriff auf diese Daten haben, diese Daten mit anderen Daten des Nutzers wie beispielsweise dem Suchverlauf, persönlichen Accounts, den Nutzungsdaten anderer Geräte und allen anderen Daten, die Google zu diesem Nutzer vorliegen, verknüpft werden.
- Der **Zugriff auf das Impressum und die Datenschutzerklärung** darf nicht verhindert oder eingeschränkt werden.

2) Technische Anforderungen an die Umsetzung des Widerrufs der Einwilligung

Beim Einsatz von Google Analytics muss stets ein einfacher und immer zugänglicher Mechanismus (z. B. Schaltfläche) zum Widerruf der einmal vom Nutzer erteilten Einwilligung implementiert sein. Gleiches gilt für Apps, die zum Beginn der Nutzung eine Einwilligung erfragen. Auch hier muss in den Einstellungen eine einfach zugängliche Möglichkeit zum wirksamen Widerruf der Einwilligung vorhanden sein.
Hatte ein Nutzer einmal seine Einwilligung erteilt und widerruft er sie zu einem späteren Zeitpunkt, so ist sicherzustellen, dass nach dem Widerruf das Google-Analytics-Skript nicht nachgeladen oder ausgeführt wird.

Google stellt ein Browser-Add-On zur Deaktivierung von Google Analytics zur Verfügung. Es ist nicht zulässig, den Nutzer ausschließlich auf dieses Add-On zu verweisen, da dies keine hinreichende Widerrufsmöglichkeit darstellt. Gemäß Art. 7 Abs. 3 S. 4 DS-GVO ist der Widerruf so einfach wie die Erteilung der Einwilligung zu gestalten. Das von Google zur Verfügung gestellte Add-On erfüllt diese Anforderungen nicht, da der Nutzer zum Herunterladen von weiteren Programmen gezwungen wird. Im Übrigen entspricht das Add-On aufgrund der Vielzahl an Browsern und Betriebssystemen weder dem Stand der Technik noch ist es geeignet, um die Datenverarbeitung in Apps zu unterbinden.

3) Transparenz

Anwender müssen gemäß Art. 13 DS-GVO die Nutzer in den Datenschutzbestimmungen umfassend über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics informieren. Bezüglich der Anforderungen an diese Informationspflicht wird auf die Leitlinie zur Transparenz[15] des Europäischen Datenschutzausschusses sowie auf die Orientierungshilfe für Anbieter von Telemedien verwiesen.

4) Kürzung der IP-Adresse

Zusätzlich zu den o. g. Maßnahmen sollten Anwender von Google Analytics durch entsprechende Einstellungen die Kürzung der IP-Adressen veranlassen. Dazu ist auf jeder Internetseite mit einer Google Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()“ zu ergänzen. Weitere Details können der technischen Anleitung von Google entnommen werden, abrufbar unter: https://developers.google.com/analytics/devguides/collection/gtagjs/ip-anonymization.

Die Kürzung der IP-Adresse stellt eine zusätzliche Maßnahme gem. Art. 25 Abs. 1 DS-GVO zum Schutz der Nutzer dar, sie führt jedoch nicht dazu, dass die vollständige Datenverarbeitung anonymisiert er-

[15] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_rev01.docx

folgt. Beim Einsatz von Google Analytics werden neben der IP-Adresse weitere Nutzungsdaten erhoben, die als personenbezogene Daten zu bewerten sind, wie z. B. Identifizierungsmerkmale der einzelnen Nutzer, die auch eine Verknüpfung beispielsweise mit einem vorhandenen Google-Account erlauben. Aus diesem Grund ist in jedem Fall der Anwendungsbereich der DS-GVO eröffnet, sodass Anwender von Google Analytics auch dann verpflichtet sind, die Anforderungen der DS-GVO zu beachten, wenn sie die Kürzung der IP-Adressen veranlasst haben. In der Datenschutzerklärung ist der Umstand, ob die Kürzung der IP-Adressen veranlasst ist, entsprechend anzugeben.

Im Übrigen gelten die Ausführungen der Orientierungshilfe für Anbieter von Telemedien.

5.13 Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 10. September 2020

I. AUSGANGSLAGE

Da eine SARS-CoV-2-Infektion teilweise mit einer spezifisch erhöhten Körpertemperatur der infizierten Person einhergeht, werden zunehmend elektronische Geräte zur Temperaturerfassung als Mittel der Zutrittssteuerung zu bis dahin öffentlich zugänglichen Räumen oder zu Arbeitsstätten eingesetzt.

Eine kontaktlose Temperaturmessung erfolgt in der Regel per Infrarotmessung und wird entweder mithilfe eines Fieberthermometers oder einer Thermalkamera / Infrarot-Wärmebildkamera[16] vorgenommen. In den nunmehr angedachten Szenarien für den Zugang zu Flughäfen, Geschäften, Behörden, Arbeitsstätten etc. wird insbesondere die Nutzung von Wärmebildkameras in Betracht gezogen, da mittels klassischer Fieberthermometer keine Temperaturmessung bei größeren Gruppen erfolgen kann. Sie kann höchstens für die Messung von Einzelpersonen nacheinander, wie z. B. in Vereinzelungsschleusen, zum Einsatz kommen, wobei bei einer einzelnen Fiebermessung mittels Thermometer ohne Protokollierung abhängig vom Einsatzszenario die Anwendbarkeit der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) in Frage stehen kann. **Einzelhandelsunternehmen und Behörden setzen bereits vergleichbare Wärmemessungen ein, um den Zutritt zu ihren Geschäftsräumen zu regulieren.**

ANWENDUNGSBEREICH DES BESCHLUSSES

Der Beschluss betrifft den Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung zur Steuerung oder aus Anlass des Zugangs zu Flughäfen, Geschäften, Behörden und Arbeitsstätten im Rahmen der Corona-Pandemie. Einrichtungen im Bereich der Gesundheitsversorgung einschließlich der Pflege können besonderen Maßnahmen unterliegen.

[16] Sofern im Folgenden allein der Einsatz von Wärmebildkameras oder der elektronischen Temperaturerfassung thematisiert wird, beziehen sich die Ausführungen grundsätzlich stets auf beide Verarbeitungsarten.

II. ZUSAMMENFASSUNG

Für die elektronische Messung der Körpertemperatur zur allgemeinen Regulierung des Zutritts zu Flughäfen, Geschäften, Behörden und Arbeitsstätten kann zwar Art. 6 Abs. 1 UAbs. 1 Buchst. e, Art. 9 Abs. 2 DSGVO i. V. m. § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutzgesetzen (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) bzw. Art. 6 Abs. 1 UAbs. 1 Buchst. f, Art. 9 Abs. 2 DSGVO (Verfolgung eines berechtigten Interesses) als Rechtsgrundlage in Betracht kommen. Auch ist die Messung als betriebliche Maßnahme des Arbeitsschutzes bzw. zur Beurteilung der Arbeitsfähigkeit gestützt auf Art. 88 DSGVO i. V. m. § 26 Abs. 3 BDSG (bzw. das Personaldatenschutzrecht des jeweiligen Landes) bzw. § 22 Abs. 1 Nr. 1 Buchst. b BDSG i. V. m. Art. 9 Abs. 2 DSGVO grundsätzlich denkbar. Jedoch fehlt es i. d. R. an der Eignung und der Erforderlichkeit der Messung. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden, und viele Infizierte weisen keine Symptome und damit auch keine erhöhte Temperatur auf. Zudem sind mildere Maßnahmen wie z. B. die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der Beschäftigten durch den Arbeitgeber denkbar.

III. DATENSCHUTZRECHTLICHE BEWERTUNG

Die elektronische Messung der Körpertemperatur fällt – jedenfalls typischerweise – in den **Anwendungsbereich** der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO).

Die Messung der Körpertemperatur eines Menschen stellt eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 und Nr. 2 DSGVO dar.

Lässt ein Verantwortlicher Körpertemperaturmessungen an Personen vornehmen, sind hierdurch regelmäßig **personenbezogene Daten** betroffen. Zwar erfassen die Temperaturmessungen selbst noch keine eindeutig identifizierenden Angaben wie Namen und Anschriften der Personen, die eine entsprechende Messeinrichtung passieren. Typischerweise kann jedoch die betroffene Person dabei anderweitig identifiziert werden, etwa durch Personal, das die Messungen und eventuell Aufzeichnungen vornimmt, durch den Einsatz von Videokameras oder durch Arbeitszeiterfassungsgeräte. Anderes könnte allenfalls gelten, wenn eine automatisierte Temperaturmessung stattfindet, die vollkommen ohne Protokollierung und ohne anderweitige Zuordnung der Werte zu bestimmten oder bestimmbaren Personen erfolgt. Im Zu-

sammenhang mit der Corona-Pandemie würde eine solche Messung allerdings ihren präventiven Zweck verfehlen.
In aller Regel sind die mithilfe einer automatisierten Temperaturmessung erzeugten Daten also personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Erst recht unterstützt die Speicherung von Infrarotkamera-Aufnahmen eine nachträgliche persönliche Identifikation betroffener Personen. Wird eine Wärmebilderfassung gar mit einer herkömmlichen Videoüberwachung verknüpft, ist generell von einem Personenbezug der Bildaufnahmen auszugehen (vgl. BVerwG, Urteil vom 27.03.2019, Az. 6C 2/18, Absatz 43 der Entscheidungsbegründung).
Die Anwendung der Datenschutz-Grundverordnung setzt nach Art. 2 Abs. 1 DSGVO weiterhin voraus, dass entweder eine automatisierte **Verarbeitung** oder eine nichtautomatisierte Verarbeitung personenbezogener Daten erfolgt, die in einem Dateisystem gespeichert werden oder werden sollen.

> Beispiel: Die Erfassung der Körpertemperatur mithilfe eines Wärmebildkamerasystems ist eine automatisierte Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO – unabhängig davon, ob die Aufnahmen gespeichert werden oder ob ein Live-Monitoring erfolgt (vgl. BVerwG, Urteil vom 27.03.2019, a.a.O., Absatz 43 der Entscheidungsbegründung).

Ausgehend von den beschriebenen Einsatzbedingungen der elektronischen Temperaturerfassung setzen die nachfolgenden Ausführungen die Anwendbarkeit der Datenschutz-Grundverordnung voraus. Sie beziehen sich allerdings nicht auf solche Temperaturmessungen, für die der Anwendungsbereich der Datenschutz-Grundverordnung ausnahmsweise nicht eröffnet ist.
Da die elektronische Temperaturmessung darauf gerichtet ist, Personen zu identifizieren, die mit SARS-CoV-2 infiziert sind, handelt es sich um eine Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO. Soweit eine solche Verarbeitung von personenbezogenen Gesundheitsdaten erfolgt, ist sie nach Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Dieses **grundsätzliche Verarbeitungsverbot** gilt nur dann nicht, wenn die Verarbeitung einen Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO erfüllt.
Im Folgenden werden daher die je nach Anwendungsfall in Betracht kommenden Rechtsgrundlagen näher untersucht, beginnend mit den allgemeinen Verarbeitungsbefugnissen.

Dabei ist neben dem grundsätzlichen Verarbeitungsverbot und den Ausnahmetatbeständen des Art. 9 DSGVO zu beachten, dass eine Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 Buchstabe a, Art. 6 Abs. 1 UAbs. 1 DSGVO nur dann rechtmäßig ist, wenn sie mindestens auf eine **Rechtsgrundlage** im Sinne des Art. 6 Abs. 1 DSGVO gestützt werden kann. Bei der elektronischen Temperaturmessung ist dies regelmäßig **nicht** gegeben. Folgende Erwägungen sind diesbezüglich zu beachten:

– Eine **Einwilligung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe a DSGVO kann nur wirksam erteilt werden, wenn die Voraussetzungen der Art. 4 Nr. 11, Art. 7 DSGVO erfüllt sind (zu Einzelheiten vgl. Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DSGVO; Europäischer Datenschutzausschuss, WP 259 rev. 01: Leitlinien in Bezug auf die Einwilligung gemäß Verordnung EU 2016/679). Zudem ist zu beachten, dass die Wärmemessung gerade der Erfassung einer etwaigen Erkrankung dient; deshalb hat die betroffene Person ihre Einwilligung ausdrücklich zu erklären (vgl. Art. 9 Abs. 2 Buchstabe a DSGVO).

  Im Zusammenhang mit der Zielsetzung der Zutrittsregulierung mithilfe von Wärmebildmessungen wird die Einwilligung als Verarbeitungsgrundlage schon in praktischer Hinsicht oft ausscheiden, weil es an der **Freiwilligkeit** der Zustimmungserklärung fehlt. Zudem wird die Wirksamkeit der Einwilligung häufig auch daran scheitern, dass eine transparente **Information** der betroffenen Person vor Durchführung des Messvorganges in der Praxis zweifelhaft scheint.

  Beispiel: Zahlreiche Beschäftigungsverhältnisse sind stark von einem Ungleichgewicht zwischen den Beschäftigten und ihrem Arbeitgeber bzw. Dienstherrn geprägt (Erwägungsgrund 43 DSGVO). Vor diesem Hintergrund werden die Beschäftigten kaum eine vom Vorgesetzten etablierte Zutrittskontrolle verweigern können, wenn sie zu ihrem Arbeitsplatz gelangen wollen. Anderes kann ausnahmsweise gelten, wenn Arbeitgeber bzw. Dienstherren etwa mithilfe von Betriebs- bzw. Dienstvereinbarungen die Rahmenbedingungen für die Freiwilligkeit einer Einwilligungserklärung von Beschäftigten festlegen.

  Beispiel: Die Zutrittsregelung betreffend Behörden- oder Gerichtsgebäuden kann typischerweise nicht auf die Einwilli-

gung gestützt werden, sofern die betroffenen Personen eine gesetzlich vorgesehene, staatliche Leistung in Anspruch nehmen wollen oder gar auf behördliche oder gerichtliche Ladung hin den Zutritt zum jeweiligen Gebäude begehren. Denn insoweit ist die Freiwilligkeit einer Zustimmung stets zweifelhaft und kann durch den Verantwortlichen regelmäßig nicht belegt werden (vgl. Art. 7 Abs. 1, Erwägungsgrund 43 DSGVO).
Beispiel: In Bezug auf den Zutritt zum Geschäftslokal eines Unternehmens wird die Einholung einer hier nach Art. 9 Abs. 2 Buchstabe a DSGVO rechtlich gebotenen ausdrücklichen Einwilligung der Kunden häufig bereits aus pragmatischen Erwägungen nicht in Frage kommen. Zudem hängt die Freiwilligkeit auch dann von den Umständen des Einzelfalls ab, wobei die gesetzliche Wertung des Art. 7 Abs. 4 DSGVO zu beachten ist.[17] Soweit der Zutritt zum Geschäftslokal an die Einwilligung zur Temperaturmessung geknüpft wird, kann also nicht ohne weiteres von einer Freiwilligkeit ausgegangen werden.

– Auch Art. 6 Abs. 1 UAbs. 1 Buchstabe b DSGVO scheidet als Rechtsgrundlage in aller Regel aus. Bei Zugangskontrollen erfolgt die Temperaturmessung nicht zur Erfüllung eines bestehenden Vertragsverhältnisses zwischen den Parteien.
Als Verarbeitungsgrundlage kommt der Vertrag am ehesten bei **Beschäftigungsverhältnissen im nichtöffentlichen Sektor und bei Tarifbeschäftigten des öffentlichen Sektors** in Betracht. Insoweit sieht Art. 9 Abs. 2 Buchstabe b DSGVO unter den dort festgelegten Voraussetzungen u. a. eine Ausnahme vom Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO vor, soweit der Verantwortliche oder die betroffene Person einer aus dem Arbeitsrecht folgenden Pflicht nachkommen muss. In Bezug auf die elektronische Temperaturmessung bei Beschäftigten kommt allenfalls in Betracht, dass mit ihr der Arbeitgeber bzw. Dienstherr seine aus dem Arbeitsschutzrecht folgenden Pflichten erfüllen will.
Eine solche vertragliche Befugnis zur Temperaturmessung kann allerdings nicht weiterreichen als eine rechtliche Verpflichtung

[17] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Rn. 14.

des Verantwortlichen im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO.

– Teilweise berufen sich Unternehmen bei der Temperaturmessung darauf, sie sei erforderlich, um eine **rechtliche Verpflichtung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO zu erfüllen. Diese Vorschrift stellt selbst keine rechtliche Verarbeitungsgrundlage dar, sondern setzt gemäß Art. 6 Abs. 2, Abs. 3 UAbs. 1 DSGVO eine Rechtsgrundlage im bereichsspezifischen EU-Recht oder im Recht eines Mitgliedstaates voraus. Die in dieser Vorschrift normierte Verpflichtung muss sich unmittelbar auf die Verarbeitung personenbezogener Daten beziehen. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus (vgl. z. B. LSG Hessen, Beschluss vom 29.01.2020, Az. L 4 SO 154/19 B, Absatz 13 der Entscheidungsgründe).
  Eine solche rechtliche Verpflichtung der Unternehmen zur Temperaturmessung ist im deutschen Recht nicht ausdrücklich vorgesehen. In Beschäftigungsverhältnissen verpflichtet § 3 Abs. 1 Arbeitsschutzgesetz den Arbeitgeber zwar allgemein dazu, die erforderlichen Maßnahmen des Arbeitsschutzes *„unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen.“* Ferner ist der Arbeitgeber nach § 618 Bürgerliches Gesetzbuch grundsätzlich verpflichtet, Maßnahmen zum Schutz von Leben und Gesundheit seiner Beschäftigten zu ergreifen. Aus diesen allgemeinen gesetzlichen Vorgaben zum betrieblichen Gesundheitsschutz lässt sich jedoch gerade nicht eine konkrete rechtliche Pflicht im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO ableiten, den Zugang zum Betriebsgelände mithilfe einer elektronischen Temperaturmessung zu regulieren.
  Auch unter Berücksichtigung des am 16. April 2020 durch das Bundesministerium für Arbeit und Soziales veröffentlichten „Arbeitsschutzstandard SARS-CoV-2“ oder der sonstigen bereichs- und branchenspezifischen Arbeitsschutzstandards ergibt sich nichts anderes. Ungeachtet dessen, dass darin Temperaturmessungen als betriebliche Maßnahme in Betracht gezogen werden sollen (II. Nr. 13 des Arbeitsschutzstandards SARS-CoV-2: *„insbesondere Fieber, Husten und Atemnot ... Anzeichen für eine Infektion mit dem Coronavirus sein (können). Hierzu ist im Betrieb*

eine möglichst kontaktlose Fiebermessung vorzusehen.“), begründen sie keine rechtliche Verpflichtung des Arbeitgebers oder Dienstherrn im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, im Wege der Fiebermessung personenbezogene Daten zu verarbeiten. Denn die Arbeitsschutzstandards SARS-CoV-2 sind kein Rechtssatz, aus denen eine rechtliche Verpflichtung folgt, sondern eine Art Leitlinie der öffentlichen Verwaltung zum Arbeitsschutz.

Damit existiert gegenwärtig keine spezifische rechtliche Verpflichtung für Verantwortliche im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, elektronische Fiebermessungen durchzuführen.

- Art. 6 Abs. 1 UAbs. 1 Buchstabe d DSGVO gestattet die Verarbeitung personenbezogener Daten, wenn sie erforderlich ist, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen. Bei der im Raum stehenden Verarbeitung von personenbezogenen Gesundheitsdaten durch elektronische Temperaturmessung muss allerdings gem. Art. 9 Abs. 2 Buchstabe c DSGVO die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande sein, ihre Einwilligung in die Verarbeitung zu geben, sodass diese Rechtsgrundlage **nicht** herangezogen werden kann.
- Hingegen kommt in einzelnen Fällen in Betracht, dass die Temperaturmessung für die Wahrnehmung einer **im öffentlichen Interesse liegenden Aufgabe** erforderlich ist, die dem Verantwortlichen übertragen wurde. Dazu stellt Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO selbst keine Verarbeitungsbefugnis dar, sondern setzt nach Art. 6 Abs. 2 und 3 UAbs. 1 DSGVO eine Rechtsgrundlage voraus. Eine solche Verarbeitungsgrundlage kann grundsätzlich auch in einer Generalklausel bestehen; insbesondere muss sie von EU-Rechts wegen nicht, wie bei der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, konkret den Verarbeitungszweck enthalten. Es genügt nach Art. 6 Abs. 3 UAbs. 2 DSGVO, wenn der Zweck der Verarbeitung erforderlich ist, um eine Aufgabe zu erfüllen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies setzt immerhin voraus, dass eine solche Aufgabe im Recht des Mitgliedstaats so klar und konkret beschrieben wird, dass aus ihr rechtssicher ein zulässiger Verarbeitungszweck abgeleitet werden kann.

Insbesondere darf die gesetzliche Zuständigkeits- und Aufgabenordnung nicht durch zu unbestimmte Verarbeitungsregeln unterlaufen werden.
Daraus folgt, dass die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 Buchstabe i DSGVO, § 22 Abs. 1 Nr. 1 Buchstabe c Bundesdatenschutzgesetz (BDSG) keine allgemeine Befugnis von Behörden für die Verarbeitung von Gesundheitsdaten begründet. Diese Vorschriften beziehen sich ihrem Wortlaut und ihrer Entstehungsgeschichte nach auf das öffentliche Gesundheitswesen und auf die Gesundheitsverwaltung.
Dient die Temperaturmessung allerdings der allgemeinen **Zutrittsregulierung zu Gebäuden der öffentlichen Verwaltung**, kommt mangels bereichsspezifischer Vorschriften der Rückgriff auf die datenschutzrechtlichen Generalklauseln in § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutzgesetzen in Betracht. Anknüpfungspunkt wäre insoweit die Aufgabe einer jeder öffentlichen Stelle, einen ordnungsgemäßen – das heißt auch für Besucherinnen und Besucher sowie Beschäftigte möglichst gefahrlosen – Dienstbetrieb zu gewährleisten. Zusätzlich muss eine Verarbeitungsbefugnis im Hinblick auf die nach Art. 9 Abs. 2 DSGVO besonders geschützten Gesundheitsdaten vorliegen (etwa, soweit anwendbar, § 22 Abs. 1 Nr. 1 Buchstabe d BDSG). Dabei ist regelmäßig der Grundsatz der Erforderlichkeit zu berücksichtigen, anhand dessen zu prüfen ist, ob das Fiebermessen tatsächlich erforderlich und zielführend zur Erreichung des Zwecks ist. Für die Prüfung der Erforderlichkeit sind Konzepte zu erstellen, die die beabsichtigten Maßnahmen und die damit verfolgten Zwecke schlüssig und nachvollziehbar darlegen. Zusätzlich haben die Behörden dabei die besonderen Regeln zum Schutz sensibler Daten zu beachten. An der Eignung und Erforderlichkeit einer elektronischen Fiebermessung bestehen allerdings erhebliche Zweifel; diese werden weiter unten im Zusammenhang mit den Ausführungen zu Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO näher erörtert.
Die Steuerung des Zutritts zu öffentlichen Verkaufsflächen von Unternehmen lässt sich hingegen regelmäßig nicht auf Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO in Verbindung mit der jeweiligen mitgliedstaatlichen Befugnisnorm stützen. **Unternehmen und andere nichtöffentliche Verantwortliche** können sich

auf diese Vorschrift nur berufen, wenn ihnen eine Verarbeitungsbefugnis im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt „übertragen“ ist. Sie müssen anstelle einer Behörde tätig werden, was einen wie auch immer gearteten staatlichen Übertragungsakt voraussetzt. Mit anderen Worten können sich Privatpersonen nicht selbst zum Sachwalter eines öffentlichen Interesses erklären. Deshalb scheidet die Wahrnehmung einer öffentlichen Aufgabe im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO für nichtöffentliche Verantwortliche gegenwärtig als Verarbeitungsgrund aus (vgl. BVerwG, Urteil vom 27.03.2019, a.a.O., Absatz 46 der Entscheidungsbegründung).

– Für Unternehmen und andere nichtöffentliche Stellen steht allerdings Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO zur Verfügung, der – verkürzt ausgedrückt – eine **Verarbeitung auf Grundlage einer Interessenabwägung** dann erlaubt, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und nicht die Interessen der betroffenen Person überwiegen. Verantwortliche des öffentlichen Sektors können sich im Rahmen ihrer Aufgabenerfüllung nicht auf diese Verarbeitungsgrundlage stützen, vgl. Art. 6 Abs. 1 UAbs. 2 DSGVO.

  Im Zusammenhang mit der elektronischen Fiebermessung ist wiederum zu beachten, dass sie als Verarbeitung personenbezogener Gesundheitsdaten nur zulässig sein kann, wenn eine Ausnahme vom grundsätzlichen Verarbeitungsverbot nach Art. 9 Abs. 2 DSGVO besteht. Eine solche Ausnahme ist jedoch allenfalls in seltenen Ausnahmefällen denkbar.

  Die Verarbeitungsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO setzt nach gefestigter Rechtsprechung drei Prüfschritte voraus (vgl. u. a. EuGH, Urteil vom 04.05.2017, Az. C-13/16, Absatz 28 der Entscheidungsgründe):

  Erstens muss die Verarbeitung ein berechtigtes Interesse verfolgen, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht das Verarbeitungsinteresse des Verantwortlichen überwiegen.

Ein **berechtigtes Verarbeitungsinteresse** ist vorliegend zu bejahen, soweit die mit der elektronischen Fiebermessung verbundene Erhebung von Daten zur Abwehr von Gefährdungen für die Belegschaft bzw. der übrigen Kundschaft und damit auch der Aufrechterhaltung des Geschäftsbetriebs dienen soll.
Die **Erforderlichkeit** der Maßnahme hingegen ist regelmäßig nicht zu bejahen. Soweit die Veröffentlichung der Datenschutzkonferenz „Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie“ insoweit für die Ermittlung der Erforderlichkeit verallgemeinerungsfähig darauf hinweist, dass – unter Beachtung des Gebots der Verhältnismäßigkeit – die *„Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern legitim sein könne, insbesondere um festzustellen, ob diese selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen oder sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben“*, beschränkt sich dies auf die zulässige Datenverarbeitung im **unmittelbaren Kontext** der mit dem Pandemiegeschehen verbundenen Gesundheitsgefahren. Vor diesem Hintergrund sind Befragungen und auch weitergehende Maßnahmen nicht generell ausgeschlossen, allerdings ist das Tatbestandsmerkmal der Erforderlichkeit im spezifischen Verarbeitungszusammenhang zu beachten.
Bei der Erforderlichkeitsprüfung ist zu beachten, dass eine erhöhte Körpertemperatur nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden kann. Sie kann auch durch zahlreiche andere Ursachen, wie etwa Erkältungen, Stoffwechsel- und Gefäßerkrankungen, Rheuma, entzündliche Prozesse bedingt sein. Zudem weisen nach Angaben des Robert-Koch-Instituts (RKI) nur etwa 41 Prozent der Infizierten einen Krankheitsverlauf mit Fieber auf; in der bis zu 14 Tage umfassenden Inkubationszeit weisen die infizierten Personen noch keine Symptome auf oder bleiben über den gesamten Infektionsverlauf vollständig symptomfrei, sind aber aufgrund der Viruslast potentielle Überträger (vgl. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Steckbrief.html#doc13776792bodyText2, Stand: 12.06.2020).

Ungeachtet dessen, dass Fieber grundsätzlich symptomatisch für eine SARS-CoV-2-Infektion sein kann, kann eine Temperaturmessung mit dem Ziel des Schutzes von Beschäftigten, Kunden oder Besuchern angesichts einer überwiegenden Anzahl symptomfreier Infektionsträger allenfalls als bedingt geeignet erachtet werden. Das RKI rät daher in seinem Epidemiologischen Bulletin 20/2020 vom 14.05.2020 von der Nutzung entsprechender Vorrichtungen an Flughäfen ab, da kein Mehrwert gesehen wird (https://www.rki.de/DE/Con-tent/Infekt/EpidBull/Archiv/2020/Ausgaben/20_20.pdf?__blob=publicationFile).
In diesem Zusammenhang kommt daher der Prüfung besondere Bedeutung zu, ob mildere, weniger eingriffsintensive Maßnahmen zur Erreichung des verfolgten Zwecks, dem Schutz der Beschäftigten und Kunden, die gleichsam der Zweckerreichung dienen, ersichtlich sind. Angesichts dessen sind die üblichen Maßnahmen im **Einzelhandel**, wie etwa die Begrenzung der Kundenanzahl, das Anbringen von Hinweisschildern zu Verhaltensregeln und Zutrittsbeschränkungen, die Gewährleistung der Einhaltung von Mindestabständen, die Aufforderung zum Tragen eines Mundschutzes, die Anbringung von Trennwänden im Kassenbereich und an Verkaufstresen sowie die Implementierung von Hygienevorgaben zu nennen. Ein derartiges Maßnahmenpaket verspricht gerade auch im Hinblick auf die größere Gefahr der Virus-Exposition aufgrund nicht festgestellter symptomfrei Infizierter einen nachhaltigeren Schutz von Kunden und Beschäftigten als eine eingriffsintensive kameragestützte Erhebung von Gesundheitsdaten.
Im Ergebnis kann daher eine Erforderlichkeit der elektronischen Fiebermessung als Instrument der Zutrittsregulierung zu öffentlichen Verkaufs- und Verkehrsflächen, insbesondere im Bereich der Grundversorgung sowie für Bereiche, deren Nutzung für das tägliche Leben unabdingbar sind (z. B. Bahnhöfe, Flughäfen, Gebäude von Verwaltungsbehörden) nicht bejaht werden.
Bei der Fiebermessung als **betriebliche Maßnahme des Arbeitsschutzes** ist zu beachten, dass ihre rechtliche Zulässigkeit aufgrund der Konkretisierungsklausel des Art. 88 DSGVO anhand des § 26 BDSG zu beurteilen ist. Für Beschäftigte des öffentlichen Sektors der Länder ist das Personaldatenschutzrecht des jeweiligen Landes maßgeblich; auf dieses wird nachfolgend aber

nicht weiter eingegangen. Im Hinblick auf die Erforderlichkeit ist zu berücksichtigen, dass der Verantwortliche als Arbeitgeber bzw. Dienstherr die Feststellung einer erhöhten Körpertemperatur mit nachfolgenden Untersuchungen kombinieren kann, was die Eignung der Maßnahme etwas erhöht. Nichtsdestotrotz ist im Hinblick auf die Erforderlichkeit zu berücksichtigen, dass symptomfreie Infektionsfälle durch eine elektronische Temperaturerfassung nicht aufgedeckt werden können. Im Übrigen bestünde – je nach Fragestellung und anlassbezogen – als mildere Maßnahme noch die Möglichkeit, nach gesundheitlichen Beeinträchtigungen der Arbeitsfähigkeit zu fragen, wenn dies wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt. Danach ist anlassbezogen die Frage nach dem Gesundheitszustand eines Beschäftigten zulässig, wenn gezielt die Beschäftigung unzumutbar machende potenzielle Ausfallzeiten oder Einschränkungen der Tätigkeit bestehen oder zu erwarten sind. Weiterhin darf allgemein nach dem Vorliegen von ansteckenden Krankheiten gefragt werden, die Kollegen oder Kunden gefährden könnten.

Bejaht man ungeachtet der vorstehenden Bedenken die Erforderlichkeit ebenso wie das Nichtüberwiegen der schutzwürdigen Interessen der betroffenen Personen, ist zu prüfen, ob das grundsätzliche Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO der Fiebermessung nicht entgegensteht. Nach den bereits gegebenen Hinweisen kommt insoweit gegenwärtig eine Ausnahme vom Verarbeitungsverbot nur noch nach Art. 9 Abs. 2 Buchstabe h DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 Buchst. b bzw. 26 Abs. 3 BDSG in Betracht. Danach ist eine Verarbeitung personenbezogener Gesundheitsdaten nicht verboten, wenn sie für die **Beurteilung der Arbeitsfähigkeit** erforderlich ist. Die Dokumentation müsste den zentralen Grundsätzen, u. a. der Zweckbindung, der Datenminimierung und Speicherbegrenzung, folgen. Zudem ist die Erfüllung der in Art. 9 Abs. 3 DSGVO, § 22 Absatz 1 Nummer 1 Buchstabe b) BDSG genannten Bedingungen und Garantien geboten. Mit anderen Worten dürfte eine elektronische Fiebermessung nur durch einen betriebsärztlichen Dienst vorgenommen werden. Dieser dürfte dem Arbeitgeber bzw. Dienstherrn allenfalls mitteilen, welchen Beschäftigten der Zutritt zum Betriebsgelände verweigert worden ist.

Im Bereich des betrieblichen Gesundheitsschutzes sind im Übrigen die Beteiligungsrechte der Interessensvertretungen zu beachten.
Die zulässige Verwendung elektronischer Temperaturmessgeräte hängt schließlich insgesamt von der Erfüllung **weiterer datenschutzrechtlicher Vorgaben** ab, z. B. sind die Regelungen zum Verzeichnis von Verarbeitungstätigkeiten, zur Datenschutz-Folgenabschätzung sowie zur Information nach Art. 12 ff. DSGVO (Hinweisbeschilderung) zu beachten.
Der Verantwortliche hat zudem dafür Sorge zu tragen, dass die Vorgaben des **Datenschutzes durch Technikgestaltung** aus Art. 25 DSGVO und der **Datensicherheit** nach Art. 32 DSGVO erfüllt werden. Hierbei können beispielsweise folgende Gesichtspunkte eine Rolle spielen:

- Geeignete Körperstellen zur Messung: Eine aussagekräftige Erfassung eines kompletten Wärmebilds eines Menschen ist kaum möglich, da z. B. die Kleidung die Infrarot-Abstrahlung verändern kann. In der Regel wird daher an der Stirn oder den Innenwinkeln der Augen gemessen. Es sind somit Spezialkameras nötig, die diese Stellen automatisiert erkennen und anvisieren können.
- Messgenauigkeit: Klassische kontaktlose Stirnthermometer haben häufig größere Abweichungen. Abhängig vom Einsatzkontext müssen daher Systeme zum Einsatz kommen, die eine deutlich höhere Messgenauigkeit haben, als übliche kontaktlose Fieberthermometer für den Hausgebrauch bieten.
- Verfälschung der Messung: Zudem muss berücksichtigt werden, dass neben anderen Erkrankungen auch körperliche Betätigung (Sport, Eile), Umgebungsbedingungen etc. zu Messunterschieden oder Abweichungen beitragen können.
- Absolute / relative Messung: Es gibt sowohl die Herangehensweise, einen Schwellwert festzulegen, ab dem die Wärmebildkamera positiv detektiert, als auch die Messung und Alarmierung im Vergleich zu den umgebenden Menschen durchzuführen. Im ersteren Fall stellt sich insbesondere die Schwierigkeit, wie der relevante Grenzwert für Fieber festzulegen ist, soweit die Körpertemperatur im Verlauf des Tages schwankt und zudem bei Kindern und Erwachsenen unterschiedlich ausfallen kann.

- Fehlerrate: Aufgrund der technischen Schwierigkeiten der Messung kann es auch unabhängig von der Problematik, dass Infizierte noch keine Symptome zeigen, zu „falsch-positiven“ wie auch „falsch-negativen“ Ergebnissen kommen, beispielsweise abhängig von der Festlegung der Schwellwerte und der Aufstellsituation.
- Auflösung, Bildgenauigkeit: Viele Wärmebildkameras bieten eine sehr hohe Auflösung, so dass sich die Frage stellt, welche zusätzlichen Informationen damit ersichtlich sind, insbesondere, wenn ein Echtbild des Gesichts in hoher Auflösung erfasst wird (Erkennung anderer Krankheiten, biometrische Identifikation etc.).
- Automatische Messung / menschlicher Bediener: Aufgrund des Aufwands für die Messung ist davon auszugehen, dass diese nicht vollautomatisiert erfolgen kann, sondern zumindest von menschlichem Personal überwacht werden muss. Zudem ist im Fall einer positiven Detektion in der Regel menschliche Intervention nötig, um die betroffene Person herauszufiltern und weitere Maßnahmen zu ergreifen.

5.14 Anwendung der DS-GVO auf Datenverarbeitungen von Parlamenten

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22. September 2020

Anlässlich des Urteils des EuGH vom 9. Juli 2020 (C-272/19) wird der Beschluss der Datenschutzkonferenz vom 5. September 2018 „Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien“ bis zur Neuformulierung eines Beschlusses ausgesetzt.

5.15 Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 26. November 2020

In der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde ein Prüfschema zum datenschutzkonformen Einsatz von Windows 10 beschlossen und anschließend veröffentlicht.[18]. Damit soll den Verantwortlichen die Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Einsatz von Windows 10 erleichtert werden. Eine Arbeitsgruppe der DSK hat unter Beteiligung von LDA Bayern, BfDI, LfDI Mecklenburg-Vorpommern und LfD Niedersachsen seitdem ihre Untersuchung von Windows 10 in Hinblick auf die Telemetriestufe Security, die in der Enterprise-Edition verfügbar ist, fortgesetzt.
Unabhängig davon hat sich das an einer Laboruntersuchung der Arbeitsgruppe neben dem LfD Bayern als Gast beteiligte BSI selbst in einer umfangreichen Studie (SiSyPHuS-Studie) auch mit Fragstellungen der Windows-10-Telemetriefunktion beschäftigt.

Untersuchungsergebnisse der DSK-Arbeitsgruppe

Die Arbeitsgruppe hat die Telemetrie von Windows 10 einer Laboruntersuchung unterzogen, um festzustellen, ob sich die Telemetriedatenübermittlung durch Konfiguration unterbinden lässt. Microsoft hat gegenüber den Aufsichtsbehörden erklärt, dass bei der Nutzung der Telemetriestufe Security keine Telemetriedaten[19] übermittelt werden.
Es wurde Windows 10 Enterprise in der Version 1909 in drei Testszenarien untersucht. In allen drei Szenarien wurden Benutzeraktivitäten simuliert, um realistische Ergebnisse zu erzielen.

1. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

[18] https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf
[19] Zum Begriff siehe Bericht Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion (Anlage 1)

2. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Basic“, 30 Minuten Testzeitraum
3. Keine Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

Die Details der Untersuchung können dem Laborbericht (Anlage 1) entnommen werden.
Die Untersuchung hat bestätigt, dass im zweiten Prüfszenario die Übermittlung von Telemetriedaten festgestellt werden konnte. Im dritten Szenario wurde ein Verbindungsaufruf zum settings-win.data.microsoft.com Endpunkt festgestellt. Dieser Endpunkt wird laut Aussage von Microsoft von mehreren Windows-10-Systemkomponenten, auch von der Telemetriekomponente, angesteuert. Nutzt die Telemetriekomponente diesen Endpunkt, besteht die Möglichkeit, dass hierüber Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten. Microsoft hat diesen Aufruf gegenüber den Datenschutzaufsichtsbehörden auf Basis eines von Microsoft zur Verfügung gestellten Laborszenarios erläutert und erklärt diesen mit einer anderen Systemkomponente abseits der Telemetrie. Microsoft hat auf mündliche Nachfrage gegenüber den Datenschutzaufsichtsbehörden erklärt, dass trotz eines – möglicherweise aufgrund eines Softwarefehlers – unbeabsichtigten Aufrufs an den settings-win.data.microsoft.com Endpunkt von dem Telemetriedienst, bei einem Telemetrielevel „Security“ weiterhin keine Telemetriedatenübermittlung stattfinden würde.

Untersuchungsergebnisse des BSI

In einer den Labortest der Arbeitsgruppe ergänzenden Untersuchung des Windows-10-Enterprise-Datenverkehrs durch das BSI im Januar 2020 wurden Datenübertragungen zu „settings-win.data.microsoft.com“ festgestellt (siehe Anlage 2).
Dabei wurde ein Windows 10 Enterprise System Version 1803 mit Telemetrielevel Security und „Windows Restricted Traffic Limited Functionality Baseline“ genutzt. Es ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com“ nicht im Klartext analysiert werden konnten und somit die Möglichkeit besteht, dass

Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt. Vor diesem Hintergrund hält das BSI aufgrund eines Defense-in-Depth-Ansatzes zur Stärkung der Sicherheit der IT-Systeme des Bundes an der Notwendigkeit einer Netztrennung von Windows-10-Clients der Bundesverwaltung, auch zur Abwehr von Schadcodes, fest.
Laut Microsoft wird über den Endpunkt „settings-win.data.microsoft.com“ auch die Konfiguration der Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ dynamisch aktualisiert.[20] Auch im BSI-Projekt „SiSyPHuS“ ist diese Adresse mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt.[21]
Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne dass der Nutzer dem zustimmen müsse oder das kontrollieren könne. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt nach der Bewertung des BSI zumindest als bedenklich einzustufen.

Konsequenzen für Verantwortliche

Im veröffentlichten Prüfschema wird erläutert, dass Verantwortliche den Nachweis für die Rechtmäßigkeit etwaiger Übermittlungen personenbezogener Daten an Microsoft erbringen oder die Übermittlung personenbezogener Daten unterbinden müssen.
Zur Unterbindung der Übermittlung personenbezogener Telemetriedaten haben die Verantwortlichen beim Einsatz der Enterprise-Edition die Telemetriestufe Security zu nutzen und mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherzustellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.
Angesichts ggf. weiterer offener Fragen, die z. B. mit dem Aufruf der „settings-win.data.micro-soft.com“-Datenverbindung verbunden sind

[20] https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
[21] https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Te-lemetry.pdf

oder die auch die SiSyPHuS-Studie des BSI aufwirft, wie des Umstands, dass die vorliegenden Untersuchungen auf Grund laufender Fortentwicklungen der Software natürlich nur eine Momentaufnahme darstellen, können die bisherigen Untersuchungen Verantwortliche nicht abschließend von ihrer aus Art. 5 Abs. 2 DS-GVO abzuleitenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst Recht für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.
Deshalb sollte Windows 10 in allen angebotenen Editionen die Möglichkeit bieten, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den in den Labor-Untersuchungen der DSK und der SiSyPHus-Studie des BSI aufgezeigten verbliebenen Unwägbarkeiten werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

Anlage 1

Die Landesbeauftragte für den Datenschutz Niedersachsen

Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion

Verantwortliche Durchführung für Tests und Dokumentation:	LfD Niedersachsen, Referat 3 - IT-Labor
Abschlussdatum der Tests:	14.05.2020
Finalisierung und Freigabe der Dokumentation:	17.06.2020

1 Zielsetzung des Tests

Microsoft gibt an, dass keine Übermittlung von Telemetriedaten an Microsoft erfolgt, wenn das Betriebssystem Windows 10 Enterprise sowie das von Microsoft zur Verfügung gestellte „Windows Restricted Traffic Limited Functionality Baseline" (V1903)[1] installiert wurde.

Ende letzten Jahres wurde bereits ein Telemetrie-Test ohne Nutzerinteraktion am Windows 10 Enterprise System (durch die *Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen)* und das *Bayerische Landesamt für Datenschutz Aufsicht (BayLDA)*) durchgeführt.

Bei diesem Test wurde festgestellt, dass die datenschutzrechtlich kontrovers diskutierten Telemetriedaten bei Einsatz der Enterprise Version im überprüften Szenario deaktivierbar sind.[2]

Da Telemetriedaten ggf. erst bei Nutzeraktivität übertragen werden, soll dieser Aspekt nun in dem vorliegenden Test berücksichtigt werden.

Dazu werden die auftretenden Datenübertragungen protokolliert (Wireshark[3]-Protokolle).

Anschließend wird untersucht, ob sich in den Protokollen Verbindungen an die von Microsoft angegebenen Endpunkte („Telemetrie-Verbindungen") finden.

Diese Endpunkte werden von Microsoft wie folgt angegeben[4]:

[1] Windows Restricted Traffic Limited Functionality Baseline: https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services, downloadlink: https://go.microsoft.com/fwlink/?linkid=828887, herunter geladen am 8.1.2020
[2] Siehe 9. Tätigkeitsbericht des BayLDA 2019: https://www.lda.bayern.de/media/baylda_report_09.pdf, Seite 22
[3] https://www.wireshark.org/
[4] https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization

Die Landesbeauftragte für den Datenschutz Niedersachsen

Windows-Version	Endpunkt
Windows 10, Version 1703 oder höher, mit installiertem kumulativen Update 2018-09	**Diagnosedaten:** v10c.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1803 oder höher, ohne kumulatives 2018-09-Update installiert	**Diagnosedaten:** v10.events.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1709 oder früher	**Diagnosedaten:** v10.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com

Verbindungen zu anderen Microsoft-Diensten, wie z. B. Windows Update Diensten, Windows Aktivierungsdienten oder Zertifikatsdiensten können ebenfalls im Wireshark Protokoll auftauchen, stellen aber keine „Telemetrie-Verbindungen" im Sinne der Definition dieses Tests dar.

Es gilt somit, herauszufinden, ob im Wireshark Protokoll Verbindungen zu den in der Tabelle aufgelisteten Microsoft Endpunkten auftauchen.

Die Landesbeauftragte für den Datenschutz Niedersachsen

Der Test beinhaltet drei unterschiedliche Prüfszenarien:

Prüfszenario 1 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 0):

- Installation des „Windows Restricted Traffic Limited Functionality Baseline". Dadurch wird u.a. der Telemetrielevel des Systems auf „0" gesetzt.
- 72 Stunden Betrieb eines Windows 10 Enterprise Systems, mit installiertem Microsoft „Windows Restricted Traffic Limited Functionality Baseline" (V1903) und verschiedenen, teilweise automatisiert ablaufenden, Benutzeraktivitäten (mit systemnahen Programmen, jeweils nach Zeitplan) innerhalb der 72 Stunden des Tests.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

Prüfszenario 2 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 1):
Laut Aussage von Microsoft ist für die tatsächliche Unterbindung der Telemetriedaten-Übermittlung das Setzen des Telemetrielevels auf „0" ausreichend.

Mit dem Prüfszenario 2 soll überprüft werden, ob bei einem Telemetrielevel größer als „0" Netzwerkverbindungen zu den von Microsoft benannten Endpunkten in den Protokollen zu finden sind.

Der Telemetrielevel kann durch folgende Registry-Einträge geändert werden:

- **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection`**
- **`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\DataCollection`**
- **`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`**

Der dort jeweils wiederzufindende Parameter *„AllowTelemetry"* bzw. *„Value"*
(in **`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`**)
stellt mit den möglichen Werten 0-3 die Intensität der Microsoft-seitigen Telemetriedaten-Übermittlung dar:

- 0 = „security" = Keine Telemetriedaten Erfassung und Übermittlung bis
- 3 = „full" = Vollständige Telemetriedaten Erfassung und Übermittlung

Anmerkung: der Telemetrielevel „0" kann in den Windows Home und Pro-Versionen von Windows 10 nicht gesetzt werden.

Die Landesbeauftragte für den Datenschutz Niedersachsen

Der Versuchsaufbau in Prüfszenario 2 wird zum Prüfszenario 1 daher nur in einem Punkt (ceteris paribus) wie folgt abgeändert:

- Der Parameter-Wert *„AllowTelemetry"* (bzw. „Value") wird manuell in den dazu verfügbaren Registrierungsvariablen auf „1" (= „einfach" bzw. „basic") gesetzt.
- Laufzeit des Tests: 30 Minuten.
  - Die verkürzte Laufzeit ist damit begründet, dass zu erwarten ist, dass in Telemetrielevel 1 bereits nach kurzer Zeit Verbindungen zu den in der o.g. Tabelle angegebenen Endpunkten (insbesondere zu *v10.events.data.microsoft.com*) stattfinden.
  - Folgende Benutzeraktivitäten am Windows 10 System werden in den 30 Testminuten durchgeführt:
    - Einstecken eines beliebigen USB Sticks.
    - Erstellen einer Notepad Datei.
    - Abspeichern der Datei auf dem USB Stick.
    - Manuelles Starten des Browsers und Aufruf der Website www.rki.de mit anschließendem Aufruf von drei Links derselben Website.
    - Schließen des Browsers.
    - Start des *Invoke User Simulators* (automatisiertes Webbrowsen).

Prüfszenario 3 (Standard-Windows-Installation, Telemetrielevel = 0):
Das in Prüfszenario 1 und 2 installierte Microsoft „Windows Restricted Traffic Limited Functionality Baseline" unterbindet nicht nur den Telemetrie-Verkehr. Es werden auch viele von Microsoft standardmäßig installierte „Zusatzprodukte" deinstalliert. Dadurch werden die Netzwerkverbindungen an Microsoftsysteme deutlich reduziert.
In manchen Fällen möchte ein Verantwortlicher aber diese „Zusatzfunktionalitäten" nutzen.

Für den Verantwortlichen wäre es also relevant zu wissen, ob die Unterbindung der Telemetrie-Datenübermittlung nur durch Setzen des Telemetrielevels auf „0" möglich ist, ohne das „Windows Restricted Traffic Limited Functionality Baseline" zu installieren und somit andere (ggf. im Unternehmensumfeld benötigte) Microsoft Dienste zu nutzen, die durch die Installation des Paketes nicht zur Verfügung stehen würden.

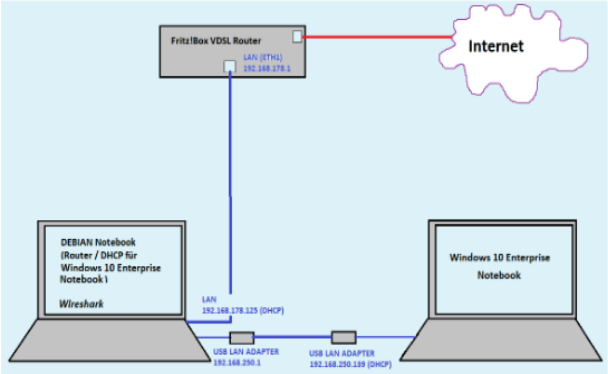
Um dies zu prüfen, wird folgender Test durchgeführt:

- Standard Installation von Windows 10 Enterprise.
- Manuelles Setzen des Telemetrielevel des Systems auf „0".
- 72 Stunden Benutzeraktivitäten am Windows 10 System, nach Zeitplan.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

Die Landesbeauftragte für den Datenschutz Niedersachsen

2 Beschreibung des Laboraufbaus

2.1 Grafische Darstellung des Laboraufbaus



2.2 Folgende Hardware Komponenten und Konfigurationen werden verwendet:

2.2.1 Notebook Lenovo Typ 20KE-S9020

Konfiguration:

- Windows 10 Enterprise V1909.
  Workgroup Installation ohne Anbindung an eine Domäne.
- Alle zum Testzeitpunkt vorhandenen Microsoft Updates werden installiert.
- Microsoft „ Windows Restricted Traffic Limited Functionality Baseline" (V1903) wird installiert (Prüfszenario 1 und 2).
- Kommandozeile: *ipconfig /flushdns* wird vor Durchführung jedes Prüfszenarios ausgeführt.
- Es werden darüber hinaus keine weiteren Veränderungen am Windows 10 Enterprise System vorgenommen.
- Das System wird vor jedem Test neu gestartet.

2.2.2 Notebook Fujitsu Typ E734 mit Betriebssystem Debian 10

Konfiguration:

- Nutzung der integrierten ETH NW Schnittstelle als Verbindung zur Fritz!Box.
- IP Adresse (192.168.178.x Bereich) wird per DHCP von der Fritz!Box an das Debian Notebook verteilt.
- Eine zusätzlich angeschlossene USB Netzwerkkarte dient als Netzwerk- Schnittstelle zum Windows 10 Enterprise Notebook.

Die Landesbeauftragte für den Datenschutz Niedersachsen

- Das Debian Notebook fungiert als Router durch Nutzung des LINUX Dienstes *dnsmasq* für das Windows 10 Enterprise Testnotebook.
- DHCP Router Dienst läuft auf Debian Notebook und vergibt IP (im Adressbereich 192.168.250.x) an das Windows 10 Enterprise Notebook.

2.2.3 Fritz!Box 7590

- Dient als Netzwerk-Router für das Debian Notebook mit V-DSL Verbindung zum Internet.
- Vor jedem Prüfszenario wird der DNS Cache der Fritz!Box geleert.

3 Beschreibung des Testablaufs

Der Test simuliert einen 72 stündigen Betrieb des Windows 10 Enterprise Notebooks.
Es werden in unterschiedlichen Zeitabständen (die minutengenau in einer Tabelle erfasst sind), am Windows 10 Enterprise Notebook manuelle Tätigkeiten mit unterschiedlichen Softwarekomponenten sowie durch ein Skript gesteuerte Browseraktivitäten vorgenommen, um Anwendertätigkeiten zu simulieren.

Dazu wird eine Teilkomponente eines automatisch ablaufenden Power-Shell Skripts verwendet. Das Skript mit dem Namen *„Invoke-UserSimulator"* wurde zur automatisierten Simulation von auf dem PC ablaufenden Vorgängen entwickelt. Es ist über *Github*[5] frei verfügbar.
Verwendet wird in diesem Test nur die Web-Browsings Funktion des Skripts.

Folgende Benutzeraktionen werden durchgeführt:

3.1 Automatisiertes Web-Browsing

Das GitHub Tool *„Invoke-UserSimulator"* startet automatisch den Browser und „klickt" skriptgesteuert automatisch in bestimmten, festgelegten Intervallen, zufällig auf Links vorgegebener (d.h. ebenfalls im Skript eingetragener) Websites, um von dort aus dann (wieder zufallsgesteuert) weiter zu browsen.
Um die im Wireshark Auswertungs-Protokoll zu erwartende Menge an IP Adressanfragen durch das automatisierte Webbrowsen nicht unnötig zu vergrößern (und so die Auswertung des Wireshark-Protokolls zu erschweren) wurde für den Test nur eine Website ausgesucht und auf dieser durch das Tool automatisiert „gesurft".
Folgende Website wurde für das automatisierte Browsen ausgewählt und verwendet, da diese Website beim Start keine Verbindungen zu anderen Host Adressen (IP Adressen) herstellt: https://www.rki.de.
Während des Testverlaufs muss zusätzlich mit dem (zufälligen) Aufruf weiterer Websites gerechnet werden, die von der Ausgangswebsite erreichbar sind.

[5] https://github.com/ubeeri/Invoke-UserSimulator

Die Landesbeauftragte für den Datenschutz Niedersachsen

3.2 Manuelle durchgeführte Tätigkeiten am Testsystem während des 72 Stunden Tests

Zusätzlich zum automatisierten Web-Browsing werden nach einem vorab festgelegten (und für spätere Erleichterung der Auswertung in einer Excel Tabelle erfassten) Zeitplan über 72 Stunden hinweg manuell folgende Aktivitäten am System durchgeführt:

- *Notepad* Datei erstellen, speichern, verändern und kopieren.
- *Systemsteuerung→ Ereignisanzeige „System" Events* zufällig auswählen und ansehen.
- *Paint Datei* (Zeichnung) erstellen, speichern, verändern und kopieren.
- Dateien mehrfach von und zu einem angeschlossenen *USB Stick* kopieren und ersetzen.

Hinweis:
Es wurden bewusst keine Drittersteller-Produkte oder Teile des Microsoft Office Pakets installiert und für die Simulation benutzt, da hier von weiterem Telemetrie-Verkehr zum Software-Hersteller auszugehen ist.

4 Auswertung der Wireshark Protokolle

Das jeweils aufgezeichnete Wireshark Protokoll des Prüfszenarios wird mittels Klartextsuche („Zeichenkette") auf das Vorhandensein der Strings

- v10c *(.vortex-win.data.microsoft.com)*
- v10. *(events.data.microsoft.com)*
- v20 (.vortex-win.data.microsoft.com)
- settings-win.data.microsoft.com

durchsucht.

Laut Microsoft wird der zu erwartende Kontakt zu den Endpunkten durch DNS-Anfragen gekennzeichnet sein (die erst außerhalb des Laborsystems bzw. des Internets, aufgelöst werden), da Microsoft die IP Adressen hinter diesen Verbindungen stetig ändert.

Im Wireshark Protokoll ist somit nur das Auffinden der oben genannten Adressen (im Klartext) entscheidend.

Die Landesbeauftragte für den Datenschutz Niedersachsen

5 Prüfergebnis

5.1 Prüfszenario 1

Im Testzeitraum von 72 Stunden konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) keine Verbindungen zu den in Kapitel 4 genannten Adressen festgestellt werden.
Eine Übermittlung von Telemetriedaten fand in diesem Szenario somit nicht statt.

5.2 Prüfszenario 2

Im Testzeitraum von nur 30 Minuten konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) bereits Verbindungen zu v10.events.data.microsoft.com und Verbindungen zu settings-win.data.microsoft.com festgestellt werden. Diese Verbindungen konnten sogar in einem zusätzlichen 30 Minuten Test ohne jegliche Benutzeraktivität festgestellt werden.
Eine Übermittlung von Telemetriedaten fand somit erwartungsgemäß statt.

5.3 Prüfszenario 3

Im Testzeitraum von 72 Stunden konnten, mit Benutzeraktivität, auf dem System (inkl. Web-Browsing) nur Verbindungen zu settings-win.data.microsoft.com festgestellt werden.
Eine Übermittlung von Telemetriedaten, insbesondere von an v10 übermittelten Diagnosedaten, hat somit nicht stattgefunden.

6 Fazit

Durch diese Tests konnten die Aussagen der Firma Microsoft nicht widerlegt werden, dass in der oben beschriebenen Konfiguration keine Telemetriedaten übermittelt werden. Hieraus kann jedoch nicht der Schluss gezogen werden, dass eine Telemetrie-Datenübermittlung grundsätzlich nicht stattfindet. Daher sind Verantwortliche stets in der Pflicht zu prüfen, ob der Einsatz von Windows 10 auch in ihrer individuellen System- und Verarbeitungssituation datenschutzrechtlich zulässig ist.

Ein besonderes Augenmerk ist auf Verbindungen zu settings-win.data.microsoft.com zu legen, da die Möglichkeit besteht, dass über diese Verbindung Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail poststelle@lfd.niedersachsen.de

Bundesamt
für Sicherheit in der
Informationstechnik

Anlage 2

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Verteiler:

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Referat 23

Bayerisches Landesamt für Datenschutzaufsicht
Bereichsleiter Cybersicherheit und Technischer Datenschutz

Die Landesbeauftragte für den Datenschutz Niedersachsen
Referat 3

Robert Krause

Bundesamt für Sicherheit in
der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582 5697
FAX +49 228 9910 9582 5697

referat-tk12@bsi.bund.de

https://www.bsi.bund.de

Betreff: Untersuchung Windows 10 Enterprise Datenverkehr

Bezug: Windows 10 Prüfung beim BayLDA am 10./11.12.2019
Geschäftszeichen: TK 12 – 240 05 00
Datum: 28.01.2020
Seite 1 von 10

Sehr geehrte Damen und Herren,

die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich mit der Frage, ob und unter welchen Konfigurationsmöglichkeiten das Betriebssystem Windows 10 von Verantwortlichen in Deutschland eingesetzt werden kann. Ein besonderes Augenmerk liegt dabei auf den sogenannten Telemetriedaten, die Windows 10 automatisch an Microsoft überträgt.

Zu diesem Thema fand am 10./11.12.2019 beim Bayrischen Landesamt für Datenschutzaufsicht ein Treffen von Behördenvertretern mit Microsoft zu einem technischen Fachaustausch statt, an dem auch das BSI aus IT-Sicherheits-Perspektive teilgenommen hat. Ziel war es, zu einer Aussage zu gelangen, ob Windows 10 Enterprise datenschutzkonform betrieben werden kann. In einem Versuchsaufbau sollte zudem nachgewiesen werden, dass keine unerwünschten Daten, insbesondere keine Telemetriedaten, mehr an Microsoft übertragen werden.

Als Ergebnis konnte festgestellt werden, dass im beobachteten Zeitraum keine Daten an Microsoft übertragen wurden, bei denen von einem besonderen datenschutz- oder it-technischen Risiko auszugehen ist. Auf Grund dessen, dass im Versuchsaufbau keine Nutzerinteraktion und weitere technische Rahmenbedingungen (z.B. Domänenmitgliedschaft und Updates) nachgebildet werden konnten, wurde das Interesse geäußert, auch diese Teilaspekte nochmals zu beleuchten.

Dies hat das BSI in einem eigenen Versuchsaufbau mit Blick auf IT-Sicherheitsaspekte getan, der im Folgenden erläutert sowie die Ergebnisse vorgestellt werden sollen.

ZUSTELL- UND LIEFERANSCHRIFT: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 2 von 10

Versuchsaufbau

Über einen Untersuchungszeitraum von 72 Stunden wurden folgende Systeme in virtuellen Maschinen betrieben:

- Router (Debian 10)
  - Einsatz als Router, DHCP-Server, DNS-Server
  - Verwendung von tcpdump zur Aufzeichnung des Netzwerkverkehrs
  - Verwendung zur live-Darstellung der Datenverbindungen

- Windows 10 Server 2019
  - Einsatz als Domaincontroller, DNS-Server, WSUS-Server
  - Bereitstellung der Gruppenrichtlinie zur Verwendung eines WSUS-Servers
  - Bereitstellung von Updates für Windows 10 SAC 1803

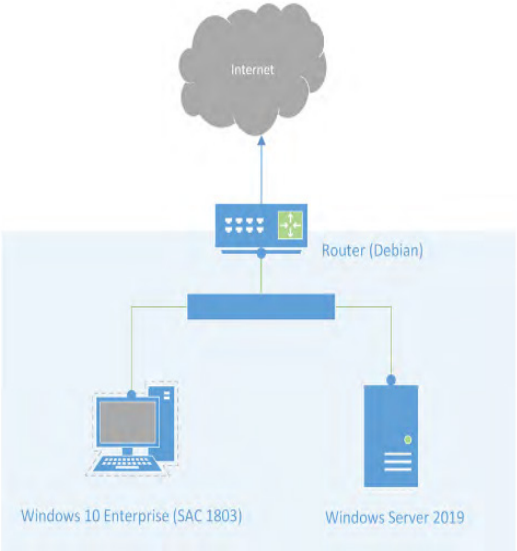
- Windows 10 Enterprise (SAC 1803)
  - Einsatz als Workstation
  - Anwendung der Windows Restricted Traffic Limited Functionality Baseline[1] für Windows 10 SAC 1803
  - Domänen-Mitglied
  - Bezug von Updates über WSUS-Server der Domäne
  - Verwendung von Fiddler und procmon zur lokalen Systemüberwachung
  - Deaktivierung des Zertifikat-Pinnings durch Setzen des Schlüssels „SkipMicrosoftRootCertCheck“ in HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Diagnostics/DiagTrack/TestHooks auf DWORD 0x1
  - Simulation von Nutzer- und Systemverhalten
    - Regelmäßige Prüfung auf Updates und deren Installation
    - Regelmäßige Neustarts
    - Simulation von Systemauslastung und Abstürzen (via Sysinternal Suite)
    - Starten und Verwenden von Programmen (ohne Internetfunktionen), z.B. Wordpad, Notepad, Powershell, Systemkommandos
    - De- und Installation weiterer Programme, Rekonfiguration der Einstellungen per GUI

1 https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 3 von 10

Das Netzwerkdiagramm stellt sich wie folgt dar:



Bundesamt
für Sicherheit in der
Informationstechnik

Seite 4 von 10

Ergebnis

Im gesamten Untersuchungszeitraum haben 2741 Pakete (1.919.128 Bytes) das Netzwerk über den Router hinaus zum Internet hin verlassen. Im Detail sind dabei folgende Endpunkte adressiert worden:

119 packets	26991 bytes	Microsoft Store Images (store-images.s-microsoft.com)	(23.210.254.117)
1931 packets	1594376 bytes	[u'www.fiddler2.com', u'fiddler2.com']	(50.56.19.116)
11 packets	2581 bytes	a2-22-119-98.deploy.static.akamaitechnologies.com	(2.22.119.98)
12 packets	2159 bytes	Microsoft.com Website (www.microsoft.com)	(23.210.253.93)
76 packets	11159 bytes	a2-22-119-33.deploy.static.akamaitechnologies.com	(2.22.119.33)
59 packets	13467 bytes	a2-22-89-31.deploy.static.akamaitechnologies.com	(2.22.89.31)
344 packets	123752 bytes	Windows Apps dynamic configuration update (settings-win.data.microsoft.com)	(40.74.35.71)
123 packets	128499 bytes	UNKNOWN	(52.155.217.156)
15 packets	3195 bytes	a2-22-94-258.deploy.static.akamaitechnologies.com	(2.22.94.250)
51 packets	14969 bytes	a2-19-241-220.deploy.static.akamaitechnologies.com	(2.19.241.228)

Diese sollen nun gesondert betrachtet werden.

50.56.19.116 – fiddler2.com – 1.6 MB / 1931 Pakete

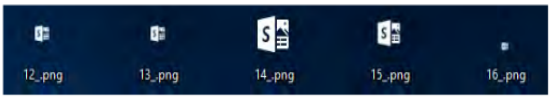
Diese IP wurde jeweils beim Starten der Anwendung „Fiddler2“ abgerufen und dient der Überprüfung und dem Bezug von Aktualisierungen. Es handelt sich um eine Verbindung, die nicht Microsoft Windows zuzurechnen ist und kann daher bei dieser Untersuchung unbeachtet bleiben.

23.210.254.117 – store-images.s-microsoft.com – 27 KB / 119 Pakete

Über den gesamten Zeitraum sind Verbindungen zum Bildarchiv des Microsoft Stores zu verzeichnen.

15	200	HTTP	store-images.microsoft.com	/image/apps.15158.9007199267163071.05e06c13-c5a6-4b55-aa49-95ac316ff92b.43c68c78-a422-4b09-acc3-77e6028d568f
16	200	HTTP	store-images.microsoft.com	/image/apps.14793.9007199267163071.55f83110-be62-4b6a-bc0a-8f12f27a5bb9.361cbfef-c19c-41d3-8a02-b1e3c8b2d188
17	200	HTTP	store-images.microsoft.com	/image/apps.63578.9007199267163071.f2756185-4638-47e0-9958-1ed9aa60f2a0.7480e404-ca1b-478b-846a-0b8514815b60
18	200	HTTP	store-images.s-microsoft.com	/image/apps.11611.9007199267163071.051d6f39-e04c-4c03-be99-103ab2771658.78beb32a-1635-487b-8355-2003309e37cf
19	200	HTTP	store-images.s-microsoft.com	/image/apps.47093.9007199267163071.afa2c461-b588-4b32-97c1-b7dadd c7d914.9e65fb00-e27b-4e87-b6aa-c6626c8503b1

Im Detail handelt es sich dabei um das Herunterladen von Bildern, u.a. von der Anwendung „Office Sway“, bei der es sich um eine Präsentations-Webanwendung handelt. Grund dafür ist vermutlich, die Anwendung als Schnellzugriff im dynamischen Startmenü von Windows anzubieten zu können.



Bundesamt
für Sicherheit in der
Informationstechnik

Seite 5 von 10

Neben den Bilddaten, sind im Rahmen der Datenverbindung folgende Informationen übertragen worden.

Request Headers

GET /image/apps.15158.9007199267163071.05e06c13-c5a6-4b55-aa49-95ac316ff92b.43c68c78-a422-4b09-acc3-77e6028d568f HTTP/1.1

Client
User-Agent: Install Service

Transport
Connection: Keep-Alive
Host: store-images.microsoft.com

Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw

Response Headers

HTTP/1.1 200 OK

Cache
Cache-Control: public, max-age=7776000, s-maxage=7776000
Date: Fri, 17 Jan 2020 09:07:24 GMT
X-Cache: MISS from dsl-ga.tn-ga
X-Cache-Lookup: MISS from dsl-ga.tn-ga:800

Entity
Content-Length: 581
Content-Type: image/png
ETag: W/"gEDUIDB4OEQyOTNDMzlGRTY1Qjc0"
Last-Modified: Fri, 24 Jul 2015 01:03:02 GMT

Miscellaneous
Accept-Ranges: none
MS-CV: a6C4E3I0SUumkJJt.0

Security
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: MS-CV

Transport
Connection: keep-alive

Diese Verbindung ist unerwartet, da davon ausgegangen wurde, dass sämtliche Verbindungen zum Microsoft Store durch Anwendung der Windows Restricted Traffic Limited Functionality Baseline unterbunden bzw. deaktiviert sind.

Dennoch geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

52.155.217.156 – displaycatalog.mp.microsoft.com – 126 KB / 123 Pakete

Im Zusammenhang mit der Überprüfung auf Updates konnten regelmäßig Verbindungen zur Domain „displaycatalog.mp.microsoft.com“ festgestellt werden, die die Grundlage zum vorher genannten Abruf der Bilddaten von „store-images.s-microsoft.com“ darzustellen scheint.

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 6 von 10

Die Kopfdaten der Verbindung stellen sich wie folgt dar:

```
Request Headers [Raw]
GET /v7.0/products/9WZDNCRD2G0J/?market=DE&languages=de-DE%2Cen%2Cneutral&fieldsTemplate=installAgent&moId=Public&oemId=Public&scmId=Public HTTP/1.1
Client
    User-Agent: Install Service
Entity
    Content-Type: application/json
Miscellaneous
    MS-CV: udKhrJUBUS3o7uV.0.2.4
Transport
    Connection: Keep-Alive
    Host: displaycatalog.mp.microsoft.com

Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML

Response Headers [Raw]
HTTP/1.1 200 OK
Cache
    Date: Tue, 21 Jan 2020 06:56:57 GMT
    Vary: Authorization
Entity
    Content-Length: 54867
    Content-Type: application/json; charset=utf-8
Miscellaneous
    MS-CorrelationId: abf0d37d-6d2a-41ed-b207-37f347aa5047
    MS-CV: udKhrJUBUS3o7uV.0.2.4.0
    MS-RequestId: 9da1f47f-4d32-481c-9820-4e6a0c220e6a
    MS-ServerId: 00002312
```

Als Antwort erhielt der Client Informationen zu von Microsoft angebotenen Produkten; hier zu Office Sway in JSON-kodierter Form.

```
Properties
    PackageFamilyName=Microsoft.Office.Sway_8wekyb3d8bbwe
    PackageIdentityName=Microsoft.Office.Sway
    PublisherCertificateName=CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

Dabei sind u.a. auch die Links zu den im Bildarchiv des Microsoft-Stores abgerufenen Icons zu finden.

```
Images
    {}
        BackgroundColor=#008272
        Caption=
        EISListingIdentifier=(null)
        FileId=2000000000045678848
        FileSizeInBytes=620
        ForegroundColor=
        Height=50
        ImagePositionInfo=
        ImagePurpose=Logo
        UnscaledImageSHA256Hash=aTdEfYnobXND4HnCTyWfc67u+7PhI4nEiedpqRFgSVM=
        Uri=//store-images.s-microsoft.com/image/apps.14185.9007199267163071.2645a823-d9a8-4e5b-a3cb-712df21f5821.dd0422a7-5158-43ff-86d4-
        Width=50
```

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 7 von 10

Auch wenn diese Verbindung unerwünscht ist und i.R. der Windows Restricted Traffic Limited Functionality Baseline nicht auftreten sollte, kann auf Grund der wenigen Daten, die der Client selbst sendet und dem Inhalt der empfangenen Daten keine Gefährdung erkannt werden.

23.210.253.93 – crl.microsoft.com – 2 KB / 12 Pakete

Hierbei handelt es sich um eine Verbindung zur Certificate Revocation List (CRL) bei Microsoft, um zu prüfen, ob Zertifikate gesperrt oder widerrufen wurden. Diese Verbindung konnte im Untersuchungszeitraum nur einmal beobachtet werden, nämlich nach dem erstmaligen Start der Anwendung „procmon". Dieses Programm ist mit einem Zertifikat signiert, um die Echtzeit nachzuweisen. In diesem Zusammenhang hat Windows offensichtlich die CRL kontaktiert.

Der nachfolgende Screenshot zeigt die Eigenschaften der Verbindung.

```
GET /pkiops/crl/MicCodSigPCA2011_2011-07-08.crl HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: www.microsoft.com

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 813
Content-MD5: w8MsPQooRx3ylPz3q1ix5w==
Last-Modified: Mon, 13 Jan 2020 06:00:56 GMT
ETag: 0x8D797EDF4BC8643
x-ms-request-id: 46820ea4-b01e-0001-12db-c9468d000000
x-ms-version: 2009-09-19
x-ms-lease-status: unlocked
x-ms-blob-type: BlockBlob
Date: Wed, 15 Jan 2020 07:03:28 GMT
TLS_version: UNKNOWN
X-RTag: RT
X-Cache: MISS from dsl-ga.tn-ga
X-Cache-Lookup: HIT from dsl-ga.tn-ga:800
Connection: keep-alive
```

Auch hier geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 8 von 10

2.22.119.98 / 2.22.119.33 / 2.22.89.31 / 2.22.94.250 / 2.19.241.220
***.deploy.static.akameitechnologies.com – 45 KB / 212 Pakete**

Bei diesen IP-Adressen und Domains handelt es sich um ein Content Delivery Network (CDN) von Akamei, das der Auslieferung und Beschleunigung von Online-Anwendungen dient. Diese Endpunkte stellen Aliase dar, den anderen, hier bereits analysierten Endpunkten entsprechen.

2.22.119.98 → crl.microsoft.com
2.22.119.33 → crl.microsoft.com

2.22.94.250 → store-images.microsoft.com
2.22.89.31 → store-images.microsoft.com
2.19.241.220 → store-images.microsoft.com

40.74.35.71 – settings-win.data.microsoft.com – 124 KB / 344 Pakete

Diese Verbindung wird vom System regelmäßig – vorrangig vor dem Überprüfen auf Windows Updates – hergestellt.

Auffällig bei dieser Verbindung war, dass sie zunächst nur auf dem Router und nicht im lokalen Proxy beobachtet werden konnte. Der per GUI / Fiddler in Windows konfigurierte Proxy-Server wurde nicht verwendet. Vielmehr war es notwendig, eine weitere Konfiguration über das Kommando „netsh winhttp set proxy" vorzunehmen.

Anschließend konnte der Aufbau der Verbindung zwar in Fiddler beobachtet werden, die Verbindung selbst hat jedoch keinerlei Nutzdaten mehr übertragen, was auf die Verwendung von Zertifikats-Pinnung durch Microsoft hindeutet.

Weitere Versuche, an den unverschlüsselten Datenverkehr zu gelangen, wurden nicht unternommen. Zu den Inhalten dieser Verbindung kann daher keine Aussage getroffen werden.

Nach Angaben[2] von Microsoft würden Apps diesen Endpunkte verwenden, um ihre Konfiguration dynamisch zu aktualisieren. So seien u.a. die Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus" und das „Windows-Insider-Programm" betroffen.

Auch im BSI-Projekt „SiSyPHuS"[3] ist diese Domain mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt. Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne

2 https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
3 https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

dass der Nutzer dem Zustimmen muss oder das kontrollieren kann. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt zumindest als bedenklich einzustufen.

Auf Nachfrage ist im Gespräch mit Microsoft am 10./11.12.2019 in Ansbach mündlich bestätigt worden, dass die in dieser Verbindungen übertragenen Daten nach Anwendung der Windows Restricted Traffic Limited Functionality Baseline (und damit des Telemetrielevels „Security") von der Windows-Telemetriekomponente nicht weiter verwendet werden würden und das Abrufen allein technische Ursachen in der Implementierung habe.

Was diese Datenverbindung tatsächlich überträgt und ob damit sicherheits- oder datenschutzrelevante Konfigurationen am System vorgenommen werden kann, mangels Einblick in den Datenverkehr, nicht bewertet werden.

Bewertung

Im Rahmen dieser Untersuchung haben sich keine Hinweise ergeben, dass Windows 10 Enterprise mit der Konfiguration „Windows Restricted Traffic Limited Functionality Baseline" Daten an Microsoft übertragen hat, die aus h.S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden.

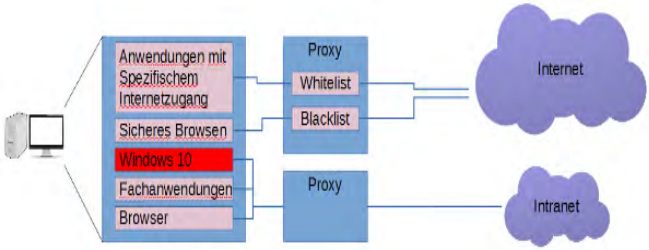
Dabei ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com" nicht im Klartext analysiert werden konnte und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt.

Darüber hinaus stellt diese Untersuchung nur eine Momentaufnahme für eine explizite Version von Windows 10 Enterprise in diesem Patchstand und einer speziellen Konfiguration dar. Durch weitere Updates und Änderungen am System durch Microsoft oder Konfigurationen des Nutzer kann sich dieses Verhalten verändern. Eine regelmäßige Aktualisierung und Prüfung der Untersuchungsergebnisse ist daher erforderlich.

Trotz der gewonnenen Erkenntnisse wird die Empfehlung des BSI, Windows 10 im Rahmen einer Netztrennung zu betreiben aufrecht erhalten. Grund dafür ist einerseits die Möglichkeit, dass sich das festgestellte Systemverhalten jederzeit durch Updates oder Konfigurationsänderungen des Herstellers ändern kann. Insbesondere die Nichtbewertbarkeit der bei der dynamischen Konfiguration der Telemetrie beteiligten Verbindung zu „settings-win.data.microsoft.com" zeigt, dass keine belastbare, abschließende Aussage möglich ist und weitere Datenkommunikation auftreten kann. Andererseits wird mit der Netztrennung eines Systems dem Grundsatz „Defence in depth" Rechnung getragen. So können nicht nur möglicherweise auftretende, unerwünschte Datenübertragungen von Anwendungen auf dem System verhindert, sondern auch wirkungsvoll die Exfiltration von Daten z.B. durch Malware vorgebeugt werden.

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 10 von 10



Dennoch bewirkt die Anwendung der Windows Restricted Traffic Limited Functionality Baseline für Windows 10 Enterprise einen deutlich verminderten Umfang an Daten, die in das Internet übertragen werden. Eine ähnliche Konfigurationsmöglichkeit auch für Windows 10 Pro/Home wäre wünschenswert.

Dabei ist jedoch – entsprechend der Benennung der Richtlinie – ein verminderter Funktionsumfang zu verzeichnen. So konnten beispielsweise im Rahmen der Untersuchung keine Anwendungen mehr gestartet werden, die Bezüge zum Windows Store haben. Die Auswirkungen auf die Praxistauglichkeit dieser Richtlinie werden auf Grund der Testergebnisse jedoch als eher gering bewertet.

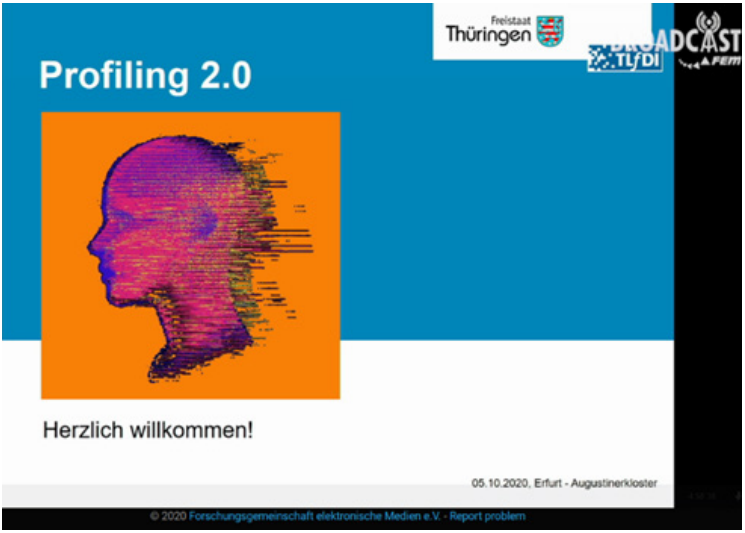
Im Auftrag

Dr. Wippig

6. Vorträge und Veranstaltungen

© Oliver Boehmer - bluedesign®- Schilder Gelb -fotolia.com

Der TLfDI informiert! Der TLfDI ist unterwegs! Datenschutz zum Anfassen! – ***doch dann kommt alles anders!*** Die Zeit der Pandemie und der Umgang mit dem Corona-Virus Sars-CoV-2 prägt auch die Öffentlichkeitsarbeit des TLfDI.
Immerhin gelingt es dem TLfDI, eine Großveranstaltung zu organisieren: „Profiling 2.0“. Die Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena zur Einführung in das Datenschutzrecht wurden ebenfalls aufgezeichnet und stehen den Studierenden im Moodle der FSU virtuell zur Verfügung.



Profiling 2.0: Wir surfen im Internet, kaufen online alles Mögliche, nutzen *zig Apps auf unseren Smartphones. Bei all diesen Aktionen hinterlassen wir unendlich viele Datenspuren im Netz. Und mit diesen Daten kann man Profile von uns Menschen erstellen. Dieses so genannte Profiling und die sich daraus ergebenden Gefahren waren Thema der Veranstaltung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) am 5. Oktober 2020 im Augustinerkloster zu Erfurt. Die Videoaufzeichnung seiner Veranstaltung „Profiling 2.0“ finden Sie unter https://femci.femnet.de/mediathek/watch/JZPLGR32CIozXoq5Izqj0/2020-10-05_TLfDI-Profiling-2.0. Die Aufzeichnung wurde durch die Forschungsgemeinschaft elektronische Medien e. V., einem studentischen Verein an der TU Ilmenau, erstellt. Alle Personen, die gefilmt wurden, gaben ihre schriftliche Einwilligung zur Aufzeichnung und der Verbreitung im Internet.
Sehen Sie in der Reihenfolge des Programms (siehe unten) die einzelnen Vorträge der Referenten zu dieser wichtigen Thematik. Zugeschaltet über eine Videokonferenz war uns Herr Professor Dr. Harald Lesch aus München, bekannt durch seine Medienpräsenz, unter anderem mit „Leschs Kosmos“ und „Frag den Lesch“. Für Frau Landtagspräsidentin Birgit Keller referierte die stellvertretende Landtagspräsidentin, Frau Dorothea Marx.

Das Programm

09:30 Einlass

10:00 Keynote des TLfDI, Herr Dr. Lutz Hasse

**10:20 Grußwort der Landtagspräsidentin,
Frau Birgit Keller,
Schirmherrin der Veranstaltung des TLfDI**

10:45 Herr Kevin Baum, Dozent Uni Saarland
„Moralische Hürden von Profiling und die Herausforderung der Erklärbarkeit": *Wir leben in einer Zeit, in der Menschen zunehmend von Software basierend auf den über sie gesammelten Daten beurteilt werden. Diese digitale Vermessung in Form von Profilen in Kombination mit der Geschwindigkeit, Verbreitung, Vielfalt und Skalierbarkeit automatischer Beurteilungen birgt diverse gesellschaftliche und moralische Gefahren.*

**11:30 Frau Katja Dittrich, alias „Letty"
& Frau Katharina Nocun**
„Ich sehe das, was du nicht siehst.": *Nach der DS-GVO sind Unternehmen verpflichtet, Auskunft über die gespeicherten Nutzungsdaten zu geben. Diese Abfragen haben einen sehr großen Datenberg zu Tage befördert. Ein Blick hinein lohnt sich. Warum dürfen Unternehmen so viel Informationen über ihre Kunden anhäufen? Und in welcher Kategorie Mensch landen wir für diese Unternehmen, ohne, dass es uns bewusst ist?*

12:30 Pause und Verteilung der Lunchpakete ☺

13:00 Herr Prof. Dr Harald Lesch, LMU München
„Homo Digitalis": *Verhaltensmuster, Einkaufsoptionen, Such-und Interessenprofile und Bewegungsprofile werden protokolliert. Der Run auf Big Data hat begonnen. Wir alle füttern bereitwillig die hungrige Datenmaschinerie mit unseren intimsten Geheimnissen.*

14:00 ***Herr Prof. Dirk Labudde,*** *Hochschule Mittweida*
„Einsatz von KI in der modernen Videoanalyse": Was Videos noch alles über Menschen verraten können. Kann man eigentlich Ansätze der künstlichen Ingerenz auch für die Ermittlungsarbeit einsetzen? Oder wiederspricht das unseren moralischen Auffassungen und Werten? Am Beispiel einer KI soll gezeigt werden, was man kann und was nicht tun sollte.

14:30 Podiumsdiskussion

Die Vortragenden

Dr. Lutz Hasse (TLfDI) legte die Juristischen Staatsexamina in Niedersachsen ab. Die Promotion erfolgte an der Universität Osnabrück während der „Jenenser Assistenz-Phase" an der FSU-Jena. 2012 und 2018 wurde er vom Thüringer Landtag zum Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

Kevin Baum ist Wissenschaftlicher Mitarbeiter und Dozent an der Universität des Saarlands. Als Dozent ist er der Kopf hinter der mit der Hochschulperle 2019 des Stifterverbands ausgezeichneten Vorlesung "Ethics for Nerds". Er ist u.a. Mitglied der Kommission für die Ethik sicherheitsrelevante Forschung und Sachverständiger der Enquetekommission Digitalisierung im Saarland. Derzeit schließt er seine Promotion zur Ethik kollektiven Handelns in Philosophie ab und arbeitet an seiner Dissertation in Informatik.

Katja Dittrich, alias Letty ist Software Entwicklerin mit Schwerpunkt Datenanalyse und -visualisierung. Ihren Datenauswertungen umfassen vielseitige Datenquellen, vom Gesamtbestand der Deutschen Nationalbibliothek bis zur Auswertung persönlicher Daten von Amazon. Ihr Wissen gibt sie als freie Dozentin weiter.

Katharina Nocun ist Wirtschafts- und Politikwissenschaftlerin. In ihrer Arbeit setzt sie sich mit dem Spannungsfeld Digitalisierung und Demokratie auseinander. In ihrem Blog kattascha.de und ihrem Podcast Denkangebot beleuchtet sie die Auswirkungen neuer Technologien für die Gesellschaft. Ihr zweites Buch (gemeinsam mit Pia Lamberty) "Fake Facts – wie Verschwörungstheorien unser Denken bestimmen" erschien im April 2020 im Quadriga Verlag.

Prof. Dirk Labudde Professor für Allgemeine und digitale Forensik an der Hochschule Mittweida und Leiter der Arbeitsgruppe FoSIL (Forensic Science Investigation Lab). Studierte Physik und Medizinphysik

Prof. Dr. Harald Lesch ist ein deutscher Astrophysiker, Naturphilosoph, Wissenschaftsjournalist, Fernsehmoderator und Hörbuchsprecher. Er ist Professor für Physik an der Ludwig-Maximilians-Universität München und Lehrbeauftragter für Naturphilosophie an der Hochschule für Philosophie München.

Moderation: Blanka Weber, sie ist freie Journalistin mit langjährigen Erfahrungen als TV-Moderatorin sowie Korrespondentin des DLF/Deutschlandradio. Sie führt durch das Programm.

„Datenschutz zum Anfassen!" ist eine neue PR-Maßnahme des TLfDI. Sie startete anlässlich des 14. Europäischen Datenschutztags am 28. Januar in der Behörde des TLfDI. **Fortsetzung folgt!** *(Nach der Pandemie)*

Unter dem Motto „Together for a better Internet" ruft die Initiative der Europäischen Kommission jährlich weltweit zu Veranstaltungen und Aktionen rund um das Thema Internetsicherheit auf. Anlässlich dieses internationalen **Safer Internet Days** am 11. Februar 2020 unterzeichneten der **TLfDI**, Dr. Lutz Hasse, und der Direktor des **Thüringer Instituts für Lehrerfortbildung, Lehrplanentwicklung und Medien**, Dr. Andreas Jantowski, einen neuen **Kooperationsvertrag** in den Räumlichkeiten des TLfDI.

Der TLfDI beteiligte sich wie jedes Jahr mit zahlreichen Vorträgen und Schulungen am **6. Datenschutztag der Karl-Volkmar-Stoy-Schule** in Jena.
Am 24. November richtete der TLfDI in seiner Funktion als Bundesvorsitzender für den Datenschutzkonferenz-Arbeitskreis Schulen und Bildungseinrichtungen eine Videokonferenz aus. Geprägt war diese virtuelle Tagung vom Thema der Pandemie. Gäste waren der Diözesendatenschutzbeauftragte und der Beauftragte für den Datenschutz der EKD in Thüringen.
Schulungen zur Datenschutz-Grundverordnung wurden auch durch zwei Fraktionen des Thüringer Landtags angefragt und vom TLfDI in 2020 umgesetzt. Geschult wurde auch für die bundesweite Innung der Schornsteinfeger, angefordert durch den Interessenverband angewandte Gebäudetechnik e. V. Ilmenau.
Die Presse- und Öffentlichkeitsstelle beantwortete circa 100 allgemeine Anfragen. Der TLfDI gab über 30 Interviews und veröffentlichte 25 Pressemitteilungen.
Die beliebte Handreichung des TLfDI zur digitalen Selbstverteidigung 2020 wurde überarbeitet und aktualisiert :-) Stand: August 2020, 7. Aktualisierung (Webversion) https://www.tlfdi.de/mam/tlfdi/presse/digitale_selbstverteidigung_auflage_7_web.pdf.
Sie kann auch gern in Papierform kostenlos bestellt werden.

7. Anhang

7.1 Vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich – Entwurf des Brexit-Abkommens bietet viermonatige Übergangsfrist ab dem 1. Januar 2021

Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 28. Dezember 2020

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist Unternehmen, Behörden und andere Institutionen in Deutschland darauf hin, dass in den Schlussbestimmungen des Entwurfs eines Handels- und Zusammenarbeitsabkommens zwischen dem Vereinigten Königreich und der Europäischen Union eine neue Übergangsregelung für Datenübermittlungen vorgesehen ist, die den bisher befürchteten gravierenden Rechtsunsicherheiten vorbeugt (Article 10A Interim provision for transmission of personal data to the United Kingdom, S. 406 ff.).
Danach sollen Übermittlungen personenbezogener Daten von der EU in das Vereinigte Königreich Großbritannien und Nordirland für eine Übergangsperiode nicht als Übermittlungen in ein Drittland (Art. 44 DSGVO) angesehen werden. Diese Periode beginnt mit dem In-Kraft-Treten des Abkommens und endet, wenn die EU-Kommission das Vereinigte Königreich betreffende Adäquanzentscheidungen nach Art. 45 Abs. 3 DSGVO und Art. 36 Abs. 3 Richtlinie (EU) 2016/680 getroffen hat, spätestens jedoch nach vier Monaten. Dieses Enddatum kann um zwei Monate verlängert werden, falls keine der beteiligten Parteien widerspricht.
Andreas Schurig: „Damit sind Übermittlungen in das Vereinigte Königreich vorerst weiterhin unter den bisherigen Voraussetzungen möglich. Gravierende Erschwernisse für die betroffenen Unternehmen werden so zunächst vermieden. Allerdings ist jetzt die EU-Kommission in der Pflicht, tragfähige Adäquanzentscheidungen vorzulegen, die auch die aktuelle Rechtsprechung des Europäischen Gerichtshofs berücksichtigen und von den Mitgliedstaaten genauso wie vom Europäischen Datenschutzausschuss sorgfältig zu prüfen sein werden.“

Stichwortverzeichnis

4-Augen-Prinzip 4.11
Abgeordneter 3.3
Akkreditierung 2.15
Altersjubiläum 3.9
Amtsblatt 3.9
Amtsgericht 2.17, 2.18
Angemessenheitsbeschluss 2.1, 2.20
Ankreuz-Formular 3.12
Anonymisierung 4.12
Anordnung 4.27
Anzeigeerstatter 2.16, 3.4
App-in-der-App 4.7
Arbeitgeber 4.24, 4.26
Arbeitnehmer 3.14, 4.24, 4.25, 4.26
Arbeitnehmerentsendegesetz 4.26
Arbeitslohn 4.26
Arbeitsunfähigkeit 4.25
Arbeitsvertrag 4.14
Arbeitszeitliste 4.26
Archiv 3.5
Arzt 3.13
Aufbewahren 2.13
Aufbewahrungsfrist 4.25
Auftragsverarbeiter 3.16
Auftragsverarbeitungsvertrag 2.3, 2.12
Auskunftei 4.17
Auskunftsrecht 2.13, 4.13
Aussonderung 3.5
Austrittsabkommen 2.20
Authentifizierung 3.2, 3.22, 4.20
Backup 3.8
Bankverbindung 2.16
Barrierefreiheit 2.14
Baugewerbe 4.26
Baumaßnahme 4.16
Beihilfe 3.19
Beihilfestelle 3.19

Beratungsanfragen 1.2
berechtigte Interessen 3.24, 4.5, 4.8
Berichtigen 2.13
Beschäftigte 4.24
Beschäftigtendaten 3.20, 3.21, 3.22, 4.14
Beschränkung der Verarbeitung 4.27
Beschwerde 1.2, 3.23
Beschwerderecht 2.18
besondere Kategorien personenbezogener Daten 4.8
Besucherraum 3.4
Betreuung 4.8
Betriebsrat 4.24, 4.25
Betriebsvereinbarung 4.24
Binding Corporate Rules 2.1
Biografiearbeit 4.15
Bonitätsabfrage 4.17
Brexit 2.20
Bundesamt für Sicherheit in der Informationstechnik (BSI) 2.10, 2.12, 3.22
Bundesmeldegesetz 3.9
Bußgeld 2.17, 3.11, 3.24
Bußgeldbescheid 1.2
Bußgeldverfahren 1.2, 2.17
Cache 3.21
Chatnachrichten 2.12
Checkliste 2.9, 2.12
Cloud-Speicher 2.7
Cookie 3.15
Corona 2.4, 4.12
Corona-Liste 1.1, 4.1
Corona-Pandemie 1.1, 2.2, 2.3, 2.5, 3.4, 3.14, 3.15, 3.22, 4.3
Corona-Verordnung 4.1
Corona-Warn-App 2.4
Cyber-Angriffe 1.2
Datenbank 3.2
Datenbankabfrage 3.2
Datenminimierung 3.19, 4.26
Datenpanne 1.2, 2.19, 3.8, 3.10, 3.11
Datenschutzbeauftragter 3.24
Datenschutzbeauftragter, betrieblicher 4.11

Datenschutzerklärung 4.23
Datenschutz-Folgenabschätzung 1.1, 2.4, 2.11, 3.15
Datenschutzkonferenz (DSK) 2.6
Datenschutzsiegel 2.15
Datensparsamkeit 2.12, 4.3, 4.23
Datenübermittlung 2.1
Datenweitergabe 4.5
Demenz 4.15
Deutsche Akkreditierungsstelle GmbH (DAkkS) 2.15
Dienstanweisung 4.10
Dienstgeheimnis 4.15
Dienstvereinbarung 3.22
digitale Gesellschaft 2.14
digitale Medien 2.3
digitale Selbstverteidigung ..... 6.
digitale Souveränität 2.8, 2.14
Digitalunterricht 1.1
Distanzunterricht 2.5, 3.16
Dokumentieren 2.13
Drittland 2.1
Drittstaatentransfer 2.6, 2.20
Drohung 3.17
EDSA 2.1
Ehejubiläum 3.9
Eheleute 3.19
Einbruch 4.29
Eingangsbestätigung 2.18
Einschränken der Verarbeitung 2.13
Einspruch 2.17
Einwilligung 2.16, 3.9, 3.16, 3.17, 3.20, 4.2, 4.4, 4.5, 4.6, 4.7, 4.9, 4.15, 4.17, 4.18, 4.19, 4.21, 4.24, 4.26
Einwohnerfragestunde 3.7
elektronische Zutrittsicherung 3.11
Eltern 3.17, 3.18
E-Mail 2.10, 2.19, 3.8, 4.6, 4.28
E-Mail-Adresse 4.9
E-Mail-Client 2.10, 4.9
E-Mail-Verteiler 2.19
Ende-zu-Ende-Verschlüsselung 2.10, 2.12, 4.28
Energieversorger 3.10

Entschließung 2.8
Entsorgungsbetrieb 2.2
Erforderlichkeit 2.16, 4.16
Ermächtigungsgrundlage 4.1
Ermittlungsverfahren 2.17
EuGH 2.1
EU-Grundrechtecharta 2.1
Europäischer Datenschutzausschuss 2.15
Europäischer Gerichtshof 1.1, 2.6, 2.20
Evaluierung 2.4
Facebook 4.7
FAQ 2.1
Fehltage 4.25
Fiebermessung 3.14
Föderalismus 2.6
Forum 4.21
Foto 4.22
Fragebogen 4.15
Framework 2.4
Freiwilligkeit 3.20, 4.26
Freizeit 4.27
Gaststätte 4.1, 4.27
Geburtstag 3.9
Gefahrenabwehr 4.27
Geheimhaltung 3.4
Gemeindeneugliederung 3.20
Gemeinschaftseinrichtung 3.18
Gerichtsvollzieher 3.6
Geschäftszeit 4.27
Gesetz gegen den unlauteren Wettbewerb (UWG) 4.6
Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Veranstaltungsrecht 4.3
Gesichtserkennung 3.15
Gesundheitsamt 2.2
Gesundheitsdaten 2.2, 3.11, 3.12, 3.14, 3.21, 3.22, 4.1, 4.11, 4.13, 4.25
Gesundheitsmanagement, betriebliches 4.24
Gewaltaufruf 3.17
Google 3.15, 3.21, 3.23
Google Maps 4.22

Google MyBusiness 4.22
Gratulation 3.9
Großbritannien 2.20
Grundversorger 4.19
Hacker-Angriffe 2.5
Handreichung 2.11
Hasso-Plattner-Institut 2.5
Haushaltsausnahme 4.29
Hinweisschild 4.29
Hochschule 3.15
hohes Risiko 2.12, 2.19, 3.10, 3.15
Homeschooling 2.3
Imbiss 4.27
Immobilienfirma 3.24
Immobilienmakler 2.17, 4.18
Impfausweis 3.12
Impfstatus 3.18
Impfung 3.18
Infektionsschutz 3.12
Infektionsschutzgesetz 2.2, 3.18
Informationspflicht 2.13, 3.15, 4.2
Inkassounternehmen 4.20
Innen- und Kommunalausschuss 3.7
Integrität 2.8, 4.20
Interessenabwägung 4.6, 4.27
Interessenausgleich 3.9
Interessenbekundung 4.17
Internetdienste 3.21
IP-Adresse 2.5
IT-Beschaffung 2.8
IT-Dienstleister 2.12
IT-Infrastruktur 2.9, 3.22
IT-Planungsrat 2.8
IT-Sicherheit 2.9
JI-Richtlinie 3.5, 3.6
Jobcenter 3.23
Justiz 3.23
Justizbereich 3.6
Kassenärztliche Vereinigung 3.13
Kategorien der personenbezogenen Daten 3.16

Kindergarten 3.12
Kindertagesstätte 3.18
Kirche 3.23
Kleine Anfrage 3.3
Kleingarten 4.29
Klinik 3.11, 4.10
Klinikarchiv 3.11
kommunale Selbstverwaltung 3.9
Kommunalordnung 3.7
Kommunalvertretung 3.7
Kommune 2.2, 2.8, 2.14, 2.16, 3.9, 3.20
Konferenz der IT-Beauftragten der Bundesressorts (KoITB) 2.8
Konformitätsbewertungsprogramm 2.15
Kontaktdaten 3.24, 4.2, 4.7, 4.19
Kontaktdatenerfassung 4.1
Kontaktformular 4.23
Kontaktnachverfolgung 4.12
Kopie 3.18, 4.13
Krankenhaus 2.1, 4.11, 4.13
Krankenhausinformationssystem 4.11
Krankheit 4.25
Krankheitsverdächtiger 2.2
Kreditwürdigkeit 4.17
kryptographische Verfahren 2.12
Kundenbewertung 4.6
Kundendaten 4.20
Kündigung 4.25
Landeskriminalamt 3.2
Landespolizeidirektion 3.2
Landgemeinde 3.20
Lastschriftverfahren 2.16
Lehrer 2.5, 3.18
Löschen 2.13
Löschung 3.5, 3.21, 4.12, 4.22, 4.29
Mahnung 3.10
Mail-Server 4.28
Mandatsträger 3.9
Masernschutzgesetz 3.18
Masernschutzimpfung 3.12
Maskenpflicht 3.17

Medienkompetenz 2.14
Medizinischer Dienst 4.15
Meldeadresse 2.18
Meldebehörde 3.9
Meldepflicht 4.19
Melderegister 3.9
Messenger-Dienst 4.14
Microsoft 2.6, 2.7
Mieter 4.16
Mieterliste 2.17
Mindestlohngesetz 4.26
mobiles Arbeiten 3.22
Mustervorlage 3.9
Nachunternehmerhaftung 4.26
nicht öffentliche Sitzung 3.7
Niederlassung 3.23
Niederschrift 3.7
Notfall 4.11
Nutzerprofil 2.12
öffentlich zugänglicher Bereich 4.29
öffentliche Stelle 2.9
öffentliche Verwaltung 2.8
Online-Dienst 3.16
Online-Meldeportal 3.24
Onlineplattformen 2.3
Online-Prüfungen 3.15
Online-Shop 4.6
Ordnungswidrigkeit 2.19
Organe der Rechtspflege 3.6
Orientierungshilfe 2.10, 2.12, 4.17
Pandemie ..... 4.1, 4.12, 6.
Passwortschutz 4.28
Patient 2.2
Patientenakte 3.11, 4.13
Patientendaten 3.13, 4.10, 4.11
Personalausweiskopie 4.18
Personalausweisnummer 4.26
Personaldaten 3.14, 4.26
Personalienaustauschkarte 3.1
Personalrat 4.11

persönliche Lebensumstände 4.3
Pfändung 3.6
Pflegebedürftige 4.15
Pflegedienst 4.14, 4.15
Plausibilitätsprüfung 3.10
Polizei 2.2, 2.17, 3.1, 3.2, 3.3, 3.4, 3.5
polizeiliche Informationssysteme 3.2
Portal 4.21
Posteingänge 1.2
Predictive Policing 3.3
Presse 3.9
Privacy Shield 2.1, 2.6, 3.16
private Krankenversicherung 4.24
Profilbildung 3.21
Profiling ..... 3.15, 6.
Protokollieren 2.13
Pseudonymisierung 4.12, 4.28
QR-Code 4.12
Qualitätsprüfung 4.15
Rechenschaftspflicht 2.9, 4.10
Rechnungshof 3.23
Recht auf Löschung 4.12, 4.21
Rechtsanwalt 4.5
Registrierung 4.21
Reichsbürger 2.18
Reisebüro 4.2
Reiseveranstalter 4.2
Religionsgemeinschaft 3.23
Restaurant 4.27
Rollen- und Rechtekonzept 4.11
Rückabwicklung von Ticketkäufen 4.3
Rückzahlungsverpflichtung 4.3
Rundfunk 3.23
Rundfunkbeitrag 3.23
Sachbeschädigung 4.29
Safer-Internet-Day ..... 6.
SARS-CoV-2 ..... 3.14
Schaden 2.19
Schadsoftware 2.19
Schenkung 4.2

Schrems II 1.1, 2.3, 2.6, 2.12, 2.20
Schrems II-Urteil 2.1
Schulcloud 2.5
Schule 2.5, 3.12, 3.16, 3.17, 3.18
Schüler 2.5, 3.17
Schulleiter 3.17
Schulrecht 3.16
Schulsoftwaresysteme 2.3
Schulung 1.1
schutzwürdige Interessen 4.2, 4.3, 4.19
Selbstauskunft 4.17
Sensibilisierung 1.1
SEPA-Mandat 2.16
Sicherheit der Verarbeitung 2.9, 3.10
Smart-City 2.14
Software as a Service 2.12
Software-Update 3.8
Sozialdaten 3.13, 3.22
soziales Netzwerk 3.21
Speicherbegrenzung 4.25
Speicherdauer 3.5, 4.29
Spracherkennung 2.7
Staatsanwalt 3.13
Staatsanwaltschaft 2.17, 3.6
Stadtbücherei 3.8
Stadtentwicklung 2.14
Stand der Technik 3.10
Standard-Datenschutzmodell (SDM) 2.9, 2.13
Standardvertragsklauseln 2.1, 2.6
Standesrecht 4.5
Statistik 1.2
Steuerbescheid 3.19
Stichproben 4.11
Straftat 2.17, 3.3, 3.5, 3.17
Straßenverkehrsordnung 3.1
Stromversorger 4.19
Suchdienst 2.7
Support 2.1
SySiPhus-Studie 2.7
Task Force 2.1, 2.6

Tatverdacht 2.17
technikneutraler Ansatz 2.11
technische und organisatorische Maßnahmen 2.7, 2.9, 2.11, 2.12, 3.8, 3.10, 3.11, 3.15, 3.16, 3.22, 4.9, 4.10, 4.20, 4.28
Telearbeit 3.22
Telefon 4.28
Telefonanlagen 2.1
Telefonnummer 4.16
Telekommunikation 3.23
Telemetrie 2.7
Testumgebung 3.8
Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien ..... 6.
Thüringer Landtag 3.7
Thüringer Schulcloud 2.3, 2.5, 3.16
Thüringer Vermessungs- und Geoinformationsgesetz (ThürVermGeoG) 3.24
ThürPolPrüffristVO 3.5
Toilette 2.17
Tonaufzeichnung 3.7
Tracing-App 2.4
Tracking-Tool 3.15
Transparenz 4.4, 4.23
Transportverschlüsselung 2.10, 2.12, 4.28
Trennen 2.13
Übermittlung 3.6
Übermittlung von Mieterdaten 4.19
Übermittlungsbefugnis 4.24
Umfrage 3.9
Unfallaufnahme 3.1
Unfallbeteiligter 3.1
Unterrichtungsanspruch des Betriebsrates 4.24
USA 2.1
Veranstaltung ..... 3.3, 6.
Verantwortlicher 3.24
Vereinigtes Königreich 2.20
Verfügbarkeit 2.8
Verkehrsunfall 3.1
Vermessungsingenieur 3.24
Vermieter 4.16, 4.19

Vernichten 2.13
Veröffentlichung 3.9
Verschlüsselung 2.10, 3.22, 4.12
Verschlüsselungskonzept 4.12
Versicherung 4.24
Versicherungsmakler 4.4
Vertragserfüllung 4.2
Vertraulichkeit 2.8, 2.10, 3.4, 4.20
Verwaltungscloud 2.8
Verwaltungsgemeinschaft 3.20
Verwarnung 2.17, 3.6, 4.4, 4.6, 4.8, 4.14, 4.16
Video 4.27
Videoaufzeichnung 3.7
Videokonferenz ..... 2.5, 6.
Videokonferenzsystem 1.1, 2.12, 3.7, 3.16
Videoüberwachung 1.1, 4.27, 4.29
Videoüberwachungsanlage 2.17
virtuelle Visitenkarte 4.22
Vollstreckungsvorgehen 3.6
Vollzugspolizei 3.5
Wahlwerbung 4.4
Webseite 4.23
Werbung 2.12, 3.15, 4.6
WhatsApp 2.17, 4.7, 4.14
WhatsBox 4.7
Widerspruch 4.24
Windows 10 ..... 2.7
Wohnungsbaugenossenschaft 4.17
Wohnungsgesellschaft 4.16
YouTube 3.23
Zertifizierung 2.15
Zertifizierungsprogramm 2.15
Zertifizierungsstelle 2.15
Zeuge 3.1, 3.4
Zugriffsrechte 4.11
Zuständigkeit 3.23
Zweckänderung 4.4
Zweckbindung 2.17, 4.23